# PC & internet prática

N.º 58 ■ Junho/Julho/Agosto 2024 ■

# SOFTWARE SECRETO GRATUITO

## Para estar 100% anónimo na Internet

## Desista do Google. Use o ChatGPT!

mais

### Faça o derradeiro exame de saúde ao seu PC

Saiba mais sobre o funcionamento interno do seu PC e detete falhas de hardware efetuando uma auditoria ao sistema

### Descubra se a sua pendrive USB é falsa

Explicamos como testar a sua pen para garantir que é realmente genuína e suporta o armazenamento que indica oferecer

# SUMÁRIO

PC & internet prática

N.º 58

Junho/Julho/Agosto 2024

**Director**
Maurício Reis

**Colaboradores**
Daniel Gomes, Eduardo Cancela, Emerson Alecrim, João Coelho, João Fernandes, João Maia, Joel Carvalho, Luís Miguel, Marco Santos, Paulo Jorge Dias, Pedro Rito

**Publicidade**
Cláudio Silva

**Marketing**
Sandra Mendes

**Redacção e Publicidade**
Rua da Escola, 35 - Coselhas
Apartado 97 - 3001-902 Coimbra
Telef./Fax: 239 081 925
Email: pceinternetpratica@gmail.com

**Impressão**
Lidergraf, SA

**Distribuição**
Vasp - Distribuição de Publicações

Publicação Periódica: 124077
Depósito Legal: 373018/14
Contribuinte: 175 282 609
Tiragem: 10.000 exemplares

A revista PC & Internet Prática é uma publicação trimestral.
Os artigos publicados são da inteira responsabilidade dos seus autores.


## FREEWARE



## PRÁTICA

# SOFTWARE SECRETO GRATUITO

## Que deve usar para se manter 100% privado na Internet

**Não comprometa a sua privacidade mantendo-se fiel às mesmas ferramentas antigas. Neste artigo, revelamos as melhores novas formas de bloquear os rastreadores da Web, proteger os seus dados e permanecer anónimo.**

A privacidade é um aspeto tão importante da nossa vida online que é frequentemente explorada para promover software que está longe de ser privado. "Mantenha a sua privacidade sob controlo", diz a página de transferência do Chrome, apesar de a Google ter sido obrigada por um tribunal a destruir os dados dos utilizadores que recolheu através do modo de navegação anónima do navegador. "Mantenha a sua privacidade online" promete o CCleaner, cuja política de privacidade afirma que "recolhe dados pessoais para personalizar anúncios para si".

Apesar de populares, estes programas prejudicam a sua privacidade em vez de a aumentarem, enquanto algumas ferramentas menos conhecidas são mais fiáveis. Em vez de recolherem e partilharem informações sobre as suas atividades na Web, protegem-no de empresas que se dedicam a práticas intrusivas, bloqueando localizadores, disfarçando a sua identidade e permitindo-lhe eliminar facilmente os seus dados privados.

Neste artigo, revelamos o melhor software secreto para se manter anónimo online, bem como destacamos novas funcionalidades e definições de privacidade ocultas em programas que poderá já utilizar.

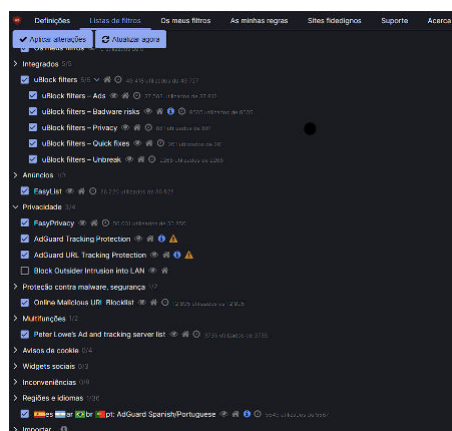
Ao contrário do modo de navegação anónima do Chrome, que não impede que os sites recolham os seus dados - como a Google agora admite - estas ferramentas funcionam exatamente como prometido, permitindo-lhe navegar discretamente na Web sem ser espiado.

Escolhemos uma mistura de software gratuito para Windows, extensões de browser e aplicações móveis para o manter 100 por cento privado em todos os dispositivos.

# BLOQUEAR TODAS AS FERRAMENTAS QUE O SEGUEM

## BLOQUEAR MAIS LOCALIZADORES NAS PÁGINAS WEB

Todos os principais navegadores da Web incluem agora proteção contra rastreio, embora alguns (Brave e Firefox) façam um trabalho muito melhor do que outros (Chrome e Edge) através das suas definições "rigorosas" ou "agressivas". No entanto, para se manter completamente privado online, bloqueando todos os rastreadores ocultos em todos os sítios Web, precisa do uBlock Origin (https://ublockorigin.com/).

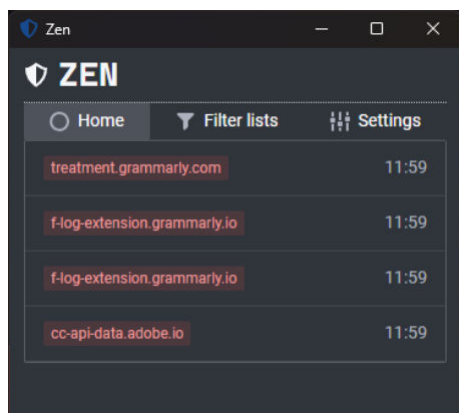
Esta brilhante extensão tem agora cerca de 55 milhões de utilizadores em todo o mundo, mas ainda não é tão conhecida como as suas rivais inferiores, como o AdBlock e o Adblock Plus. Mesmo que já utilize o uBlock Origin para bloquear anúncios e rastreadores, pode não se aperceber que tem opções adicionais para bloquear outros riscos de privacidade.

**Melhore a proteção de rastreamento do uBlock Origin adicionando filtros do AdGuard**

Clique com o botão direito do rato no botão da barra de ferramentas do complemento, selecione 'Opções' e clique no separador 'Listas de filtros'. Clique na seta junto a 'Privacidade' e assinale as caixas 'AdGuard Tracking Protection' (Proteção de Rastreio AdGuard) e 'AdGuard URL Tracking Protection' (Proteção de Rastreio URL AdGuard) - bem como 'EasyPrivacy' (Privacidade Fácil), se não estiver ativada. Estes filtros aumentam os filtros do uBlock Origin com regras do serviço freemium AdGuard para fornecer uma proteção abrangente e constantemente atualizada contra os mais recentes rastreadores - incluindo os escondidos em endereços Web. Clique em 'Aplicar alterações' e depois em 'Atualizar agora'.

Infelizmente, o novo sistema Manifest V3 da Google, que será introduzido este ano, limitará os bloqueadores de conteúdos a 30.000 regras de filtragem - o uBlock Origin utiliza atualmente cerca de 300.000 - o que os tornará menos eficazes no bloqueio de anúncios e de rastreadores. Para ultrapassar esta restrição, o uBlock Origin criou uma versão Lite para o Manifest V3 (https://tinyurl.com/69udthcc) que permite configurar os seus filtros site a site, escolhendo entre os modos de filtragem Básico, Ótimo ou Completo.

## BLOQUEAR RASTREADORES NO SOFTWARE WINDOWS

Ferramentas como o uBlock Origin facilitam o bloqueio de rastreadores no seu navegador, mas é mais difícil evitá-los noutros softwares do seu PC. Muitos programas incluem agora elementos de rastreio que se ligam à Internet em segundo plano para partilhar detalhes das suas atividades com programadores, anunciantes e corretores de dados - e potencialmente criminosos.

Pode bloquear estes rastreadores ocultos utilizando uma nova ferramenta

**O ZEN define um 'proxy' para bloquear as requisições de rastreamento no software do Windows**

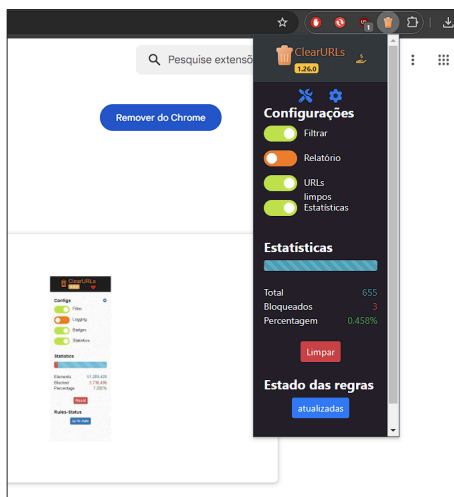
de código aberto chamada Zen (https://tinyurl.com/2zzdjddf - vá à secção Download na descrição do programa), não relacionada com o Zen Internet. Este bloqueador de anúncios e protetor de privacidade gratuito cria um proxy que intercepta os pedidos de rastreio dos servidores da Internet e bloqueia todos os que contenham anúncios, scripts de rastreio, malware e outros conteúdos indesejados. Ao trabalhar ao nível do sistema, o Zen protege o seu PC contra ameaças que as extensões do navegador não detetam, como os rastreadores incorporados no software do Windows e nos componentes do sistema.

Descarregue e execute o instalador x64 ou a versão portátil do Zen, clicando em "Mais informações" e depois em "Executar na mesma" quando vir o aviso do Microsoft Defender SmartScreen - é totalmente seguro. Quando abrir o programa pela primeira vez, clique em 'Iniciar' ('Start') e depois em 'Sim' ('Yes') para instalar o seu certificado de raiz, que lhe permite verificar e modificar os pedidos HTTPS - este certificado é gerado e armazenado de forma privada no seu PC.

Uma vez feito isto, o Zen começará a mostrar os pedidos bloqueados no seu separador Home. Para aumentar a sua proteção, clique no separador 'Listas de filtros' ('Filter Lists') e ative a 'Lista de servidores de anúncios e rastreio de Peter Lowe' ('Peter Lowe's Ad and tracking server list') - outros filtros podem ser ativados no menu pendente. Se tiver problemas em carregar um determinado sítio Web ou programa, clique em 'Parar' ('Stop') para se desligar do proxy.

Embora o Zen não seja tão potente como soluções pagas, como o AdGuard (https://tinyurl.com/2up9rytv), é fácil de usar e não precisa de se registar com uma conta.

## REMOVER ELEMENTOS DE RASTREIO DOS ENDEREÇOS URL

Muitos URLs em sítios Web - incluindo resultados de pesquisa do Google, páginas de produtos da Amazon e publicações em redes sociais - contêm código adicional após o endereço Web principal. Normalmente, isto serve para fins analíticos, para informar os proprietários do sítio quando clicou na ligação, o país a partir do qual está a navegar e o dispositivo que está a utilizar, mas o código também pode ser utilizado para o localizar na Internet.

**O ClearURLS remove código de rastreamento dos endereços da Internet (URLs) incluindo resultados da pesquisa do Google**

Para evitar que isto aconteça, instale a extensão ClearURLs no seu navegador Chromium (https://tinyurl.com/2a8k8wpm) ou Firefox (https://tinyurl.com/4uxb6fes). Esta extensão protege a sua privacidade, removendo automaticamente os elementos de rastreio dos URLs e permitindo-lhe clicar nas páginas sem ser redirecionado através de um serviço de terceiros.

Pode ver quantos elementos a extensão bloqueou clicando no botão da barra de ferramentas e verificando a secção 'Estatísticas' ('Statistics') no painel de informações. Se o ClearURLs impedir que alguns sites sejam carregados corretamente, clique na engrenagem 'Definições' ('Settings') e desative 'Permitir o bloqueio de domínios' ('Allow domain blocking').

A propósito, o Brave e o Firefox permitem-lhe agora remover elementos de rastreio quando copia ligações de páginas Web. No primeiro, clique com o botão direito do rato na hiperligação e escolha 'Copiar hiperligação limpa' ('Copy clean link'); no segundo, selecione 'Copiar hiperligação sem rastreio do site' ('Copy Link Without Site Tracking').

## NÃO SE DEIXE ENGANAR POR POP-UPS DE CONSENTIMENTO DE COOKIES

Os pop-ups de consentimento de cookies destinam-se a dar-lhe mais controlo sobre os dados que os sítios Web recolhem sobre si, mas são muitas vezes tão confusos que acaba por concordar em ser rastreado. A popular extensão I Don't Care About Cookies resolve o problema destes pop-ups ocultando-os automaticamente, mas também permite que os sítios instalem cookies.

Consent-O-Matic é uma alternativa menos conhecida, mas mais privada, que rejeita todos os cookies por defeito

**O Consent-O-Matic rejeita 'cookies' de rastreamento enquanto permite os essenciais**

e oculta os banners de consentimento. Disponível para os navegadores Chromium (https://tinyurl.com/5xdzurvc), Firefox (https://tinyurl.com/288y7szb) e Safari no iOS (https://tinyurl.com/3p6npwdv), permite-lhe configurar as definições para permitir cookies essenciais e bloquear os de rastreio.

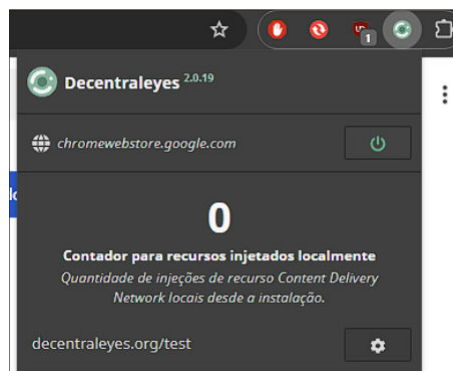
Clique no botão da barra de ferramentas, escolha 'Mais definições do Add-on' ('More Add-On Settings') e, no separador 'Sua Escolha' ('Your Choice'), selecione as categorias de cookies que pretende permitir. Por exemplo, 'Preferências e Funcionalidade' ('Preferences and Functionality') permite que os sítios armazenem dados como os seus detalhes de início de sessão e definições de personalização, enquanto que 'Seleção, exibição e relatório de anúncios' ('Ad selection, delivery, and reporting') lhes dá permissão para o rastrear.

Pode adicionar regras adicionais ao Consent-O-Matic para melhorar a sua deteção e bloqueio de pop-ups de cookies. Clique no separador "Rule Lists" (Listas de regras) e copie o URL de uma lista de regras para a caixa "Add List" (Adicionar lista) - obtenha a utilizada pelo I Don't Care About Cookies em https://tinyurl.com/yhdm3jbs.

## IMPEDIR QUE AS REDES DE DISTRIBUIÇÃO DE CONTEÚDOS O MONITORIZEM

Atualmente, muitos sítios Web dependem de serviços de terceiros para fornecer alguns dos seus conteúdos, incluindo imagens, vídeos e tipos de letra. Conhecidos como redes de distribuição de conteúdos (CDN), estes serviços ajudam a acelerar o tempo de carregamento das páginas, mas também podem rastreá-lo na Web. Isto porque, depois de ver o seu conteúdo num sítio, podem segui-lo até ao sítio seguinte que utilize a sua rede.

Bloquear CDNs pode causar a quebra de sites, mas pode impedir que eles o sigam instalando o Decentraleyes no seu navegador Chromium (https://tinyurl.com/bddpcx92) ou Firefox (https://tinyurl.com/52n7u87c). Esta extensão elimina o intermediário CDN, enganando os sítios Web para que carreguem os seus próprios ficheiros armazenados localmente para apresentar o conteúdo.

Ao fazê-lo, a Decentraleyes protege a sua privacidade sem afetar a sua

**O Decentraleyes substituiu, com os seus próprios ficheiros, conteúdo da Internet que pode rastrear o utilizador**

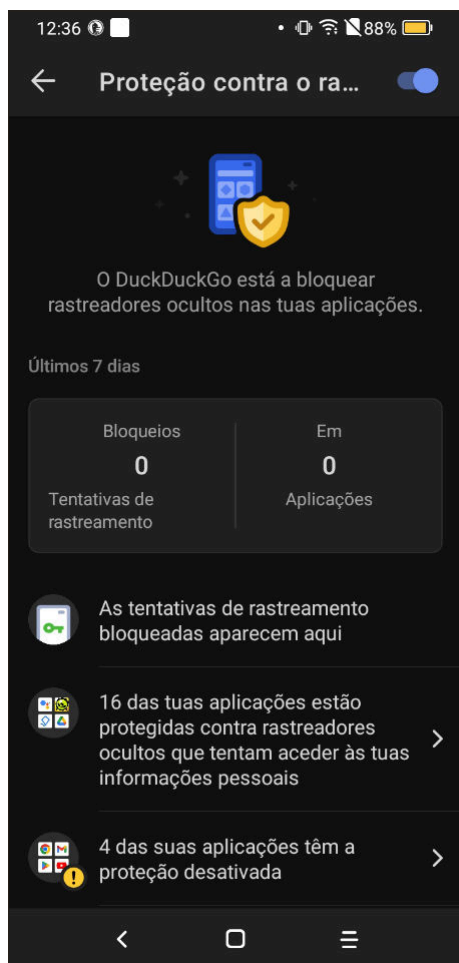
navegação - pode ver quantos recursos substituiu nas páginas clicando no botão da barra de ferramentas.

Funciona em conjunto com bloqueadores de conteúdos, como o uBlock Origin, e sem que seja necessário configurar as suas definições. Se tiver problemas em carregar um site, clique no botão de ligar/desligar para desativar a proteção do suplemento.

## BLOQUEAR RASTREADORES OCULTOS EM APLICAÇÕES MÓVEIS

Alguns rastreadores incorporados em aplicações móveis recolhem dados sobre as suas atividades para partilhar com anunciantes e outras empresas, não só nas próprias aplicações, mas também noutras aplicações instaladas no seu telemóvel ou tablet. É por isso que é frequente ver anúncios e conteúdos patrocinados relacionados com coisas que viu numa aplicação aparecerem numa ferramenta completamente diferente.

O excelente DuckDuckGo Private Browser para Android (https://tinyurl.com/bdeeafd4) evita que isto aconteça utilizando a sua funcionalidade de proteção contra o rastreio de aplicações. Para além de bloquear os rastreadores ocultos nos sites que visita no navegador, recusa os pedidos de rastreio noutras aplicações no seu dispositivo Android. Isto impede que estas recolham dados sobre si, ao mesmo tempo que permitem as permissões de que necessitam para funcionar.

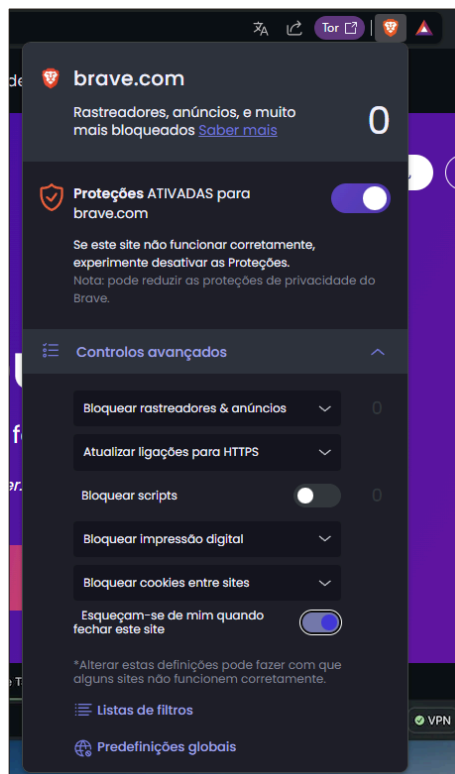
Para ativar a funcionalidade, toque no menu de três pontos no DuckDuckGo Private Browser, selecione 'Definições' ('Settings') e ative 'App Tracking Protection' ('Proteção contra o rastreamento por aplicações'). Toque em 'OK' para permitir que o DuckDuckGo configure uma VPN no

**O navegador para Android DuckDuckGo não permite que apps rastreiem o que faz noutras apps**

seu dispositivo - não se trata de uma VPN propriamente dita, mas permite que o browser bloqueie os rastreadores ao nível da rede. O DuckDuckGo indica-lhe quantas tentativas de rastreio foram bloqueadas em aplicações nos últimos sete dias, bem como as aplicações e as empresas de rastreio responsáveis.

O navegador iOS do DuckDuckGo (https://tinyurl.com/zpvmkbsv) não inclui esta funcionalidade, mas o seu iPhone (ou iPad) tem a sua própria definição para bloquear o rastreio de aplicações. Selecione 'Privacidade e segurança' na app 'Definições', toque em 'Seguimento' e desative a opção 'Permitir pedidos de seguimento das aplicações'. Quando esta opção está desativada, todos os novos pedidos de rastreio de aplicações são automaticamente recusados.

# TORNE-SE INVISÍVEL ONLINE

## FAÇA COM QUE OS SÍTIOS WEB SE ESQUEÇAM QUE OS VISITOU

Não é segredo que o modo incógnito ou privado do seu browser não o mantém nem de perto nem de longe anónimo online - como a Google foi recentemente forçada a esclarecer. Mas a Brave (www.brave.com) tem agora uma funcionalidade secreta chamada 'Forget by Default' (Esquecer por defeito), que vai mais longe do que os modos de navegação privada normais, impedindo que os sítios Web o identifiquem.

**Use a nova opção do Brave 'Forget by Default' (numa tradução livre, Esquecer por Defeito) para que os websites parem de o identificar**

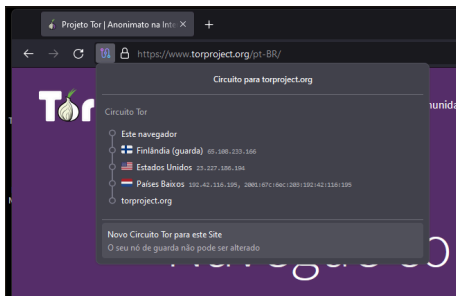
O 'Forget by Default' funciona fazendo o logout de um site e apagando todos os seus cookies e outros dados armazenados quando se fecha o separador do navegador. Isto significa que, da próxima vez que visitar esse sítio, este não o reconhecerá automaticamente e não adaptará o seu conteúdo - e anúncios - em conformidade.

Para aceder a esta funcionalidade, clique no botão 'Shields' (cabeça de leão) na barra de ferramentas do Brave e ative a opção 'Forget me when I close this site'. Isto irá desconectá-lo e eliminar todos os cookies e outros dados assim que fechar o separador atual.

Para ativar a opção 'Esquecer por defeito' para todos os sites que visitar, clique no botão do menu de três linhas do Brave, escolha 'Definições' ('Settings'), depois 'Escudos' ('Shields') e ative a opção 'Esqueçam-se de mim quando fechar este site' ('Forget me when I close this site'). Pode desativar a opção em sites específicos, para impedir que estes iniciem sessão, clicando no botão Shields e desativando-a.

Visite brave://settings/content/all para confirmar que a opção 'Esquecer por defeito' está a limpar os dados armazenados quando sai de um site (podem permanecer alguns cookies não removíveis).

## NAVEGAR NA WEB DE FORMA ANÓNIMA UTILIZANDO O TOR

O Brave também tem um modo de navegação privada que utiliza a rede Tor para impedir que os sítios Web o

**O navegador TOR redireciona a sua ligação à Internet através de uma rede global de relés**

rastreiem e identifiquem. Recentemente, melhorou este modo carregando automaticamente o endereço onion dos sites quando disponível, e redireccionando-o para o Tor quando tenta visitar um endereço onion no modo de navegação normal. No entanto, para se manter completamente anónimo online, deve utilizar o navegador Tor dedicado (https://tinyurl.com/5eb5pe5z), que funciona em modo de navegação privada permanente.

O navegador Tor redireciona a sua ligação à Internet através de um circuito encriptado de "retransmissores" em todo o mundo, o que impede que os sítios Web, os piratas informáticos e outros bisbilhoteiros vejam onde se encontra e o que faz online. Elimina automaticamente os cookies, os dados dos sítios e o histórico de navegação quando o fecha, não deixando qualquer vestígio das suas atividades e oferece uma escolha de níveis de segurança para desativar as funcionalidades da Web que comprometem o seu anonimato.

No ano passado, o Tor simplificou o sistema de circuitos do navegador para facilitar a verificação dos relés (também designados por nós) através dos quais a sua ligação está a ser desviada para disfarçar o seu endereço IP. Clique no ícone do Circuito Tor (linha ondulada) à esquerda da barra de endereço para ver as localizações e os endereços IP de cada nó. Se suspeitar que o seu anonimato foi comprometido, talvez por ter introduzido informações pessoais num sítio Web, clique em 'Novo circuito Tor para este Site' ('New Tor circuit for this site') para ser redirecionado através de uma nova série de relés.

O Tor introduziu recentemente uma poderosa funcionalidade de privacidade chamada WebTunnel, que impede qualquer pessoa - incluindo o seu ISP - de saber que está a utilizar a sua rede encriptada.

Embora o Navegador Tor permita aceder à chamada dark web, é necessário introduzir endereços onion de 56 caracteres para visitar esses sites, para que não se depare acidentalmente com algo ilegal. Além disso, muitos sítios Web de renome, incluindo a BBC News, o Guardian e a Amnistia Internacional, têm versões onion para ajudar os visitantes a vencer a censura e a vigilância. A principal desvantagem é que o carregamento de sites padrão pode ser lento - especialmente no nível de segurança 'Mais seguro' ('Safest') do navegador.

O navegador Tor também tem uma aplicação para Android (https://tinyurl.com/4663v6hk) que lhe permite navegar anonimamente na Web no seu telemóvel ou tablet. As restrições da Apple impedem-no de funcionar num iPhone ou iPad, pelo que o Tor recomenda que combine o Onion Browser (https://tinyurl.com/5ewpwaau), que foi "desenvolvido por alguém que trabalha em estreita colaboração com o Projeto Tor", com a sua VPN Orbot (https://tinyurl.com/k79wwmyz).

## OCULTE AS SUAS ATIVIDADES ONLINE COM UMA VPN GRATUITA

Uma rede virtual privada (VPN) é a forma mais fiável de aceder à Web de forma anónima, porque encripta a sua ligação à Internet em todo o dispositivo e não apenas no seu navegador (como faz o navegador Tor). No entanto, as subscrições de VPN podem ser dispendiosas e os serviços gratuitos têm normalmente inconvenientes - desde limites de dados apertados e má escolha de servidores a políticas de privacidade duvidosas que lhes permitem recolher e partilhar os seus dados.

Uma das melhores opções é a versão gratuita do Proton VPN (https://tinyurl.com/5emf5ymh), que oferece dados mensais ilimitados, sem anúncios e com uma política rigorosa de não registo de dados. Possui um "kill switch" que o coloca automaticamente offline quando perde a ligação encriptada, para que o seu anonimato nunca seja comprometido, e um "modo furtivo" que disfarça o facto de estar a utilizar uma VPN. No entanto, este modo está atualmente disponível apenas nas aplicações móveis e macOS, não no programa Windows.

Anteriormente, o plano gratuito do ProtonVPN permitia-lhe escolher entre servidores na Holanda, Japão e EUA, mas agora atribui um aleatoriamente quando clica nos botões 'Ligação rápida' ('Quick Connect') ou 'Trocar servidor' ('Change server').

Isto torna-o menos útil para desbloquear conteúdos com restrições geográficas do que para disfarçar as suas atividades online, embora tenha recentemente adicionado servidores gratuitos na Polónia e na Roménia.

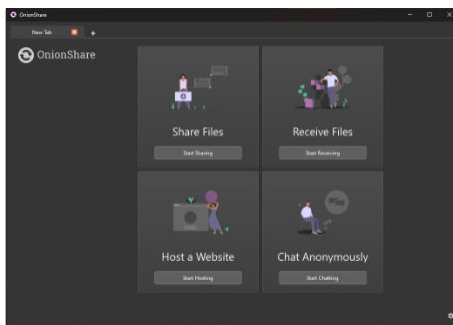
**O ProtonVPN é uma das poucas VPNs gratuitas que oferece dados mensais ilimitados**

Atualizar para ProtonVPN Plus por €4,99 por mês dá acesso a mais de 4.500 servidores em mais de 90 países e permite que use o serviço em até 10 dispositivos (a versão gratuita limita você a um).

Em alternativa, a VPN gratuita da Windscribe (https://tinyurl.com/bd9hmt25) oferece 10 GB de dados por mês (2 GB até confirmar o seu endereço de correio eletrónico) e acesso a servidores em 10 países, incluindo os EUA, Reino Unido, Canadá, França, Alemanha e Hong Kong. O seu modo furtivo está disponível nas suas aplicações para computador e telemóvel e a sua funcionalidade 'split tunnelling' permite-lhe excluir programas específicos da sua proteção.

### PARTILHAR E RECEBER FICHEIROS ANONIMAMENTE

Pode utilizar o navegador Tor - ou uma VPN - para descarregar ficheiros de sítios Web sem revelar a sua identidade ou localização, mas é menos fácil partilhar ficheiros sem comprometer a sua privacidade. Para isso, precisa da ferramenta gratuita OnionShare (https://tinyurl.com/ycys2pfa), que lhe permite enviar e receber ficheiros de forma segura e anónima através da rede Tor.

Instale a aplicação OnionShare no seu PC (também está disponível para macOS, Linux, Android e iOS), clique em 'Connect to Tor' e selecione 'Start Sharing' no mosaico 'Share Files'. Adicione os ficheiros ou pastas que pretende partilhar e clique em 'Start sharing'. Isto irá gerar um endereço onion que o destinatário pretendido pode introduzir no Navegador Tor para aceder aos itens partilhados - clique em 'Copy Address' para o colar num e-mail encriptado ou numa mensagem de chat. Também é necessário enviar à outra pessoa a chave privada gerada pelo OnionShare, para que ela possa desbloquear o download. Clique em 'Stop sharing' para remover os ficheiros depois de descarregados.

**O OnionShare deixa que partilhe e receba ficheiros de forma privada através da rede Tor**

Para permitir que alguém lhe envie ficheiros através do Navegador Tor, clique em 'Start Receiving' no separador 'Receive Files', depois em 'Start Receive Mode' para gerar outro endereço onion e chave privada. A pessoa pode então introduzi-los no navegador para enviar ficheiros para si.

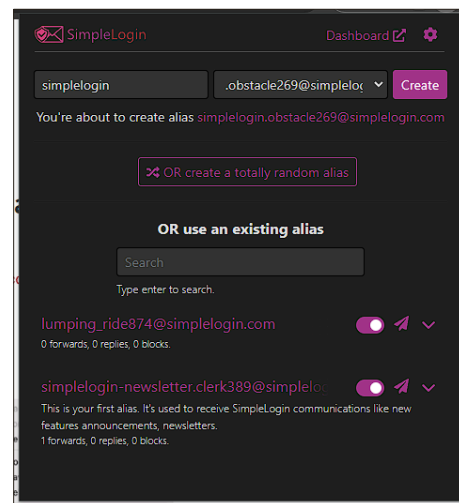
Pode parecer uma forma complicada de fazer as coisas, mas o OnionShare é fácil de utilizar e garante que nenhum terceiro pode intercetar os ficheiros que está a partilhar - ou detetar onde você e a outra pessoa estão localizados.

## PROTEJA OS SEUS DADOS PRIVADOS

### FALSIFIQUE O SEU ENDEREÇO DE CORREIO ELETRÓNICO UTILIZANDO UM PSEUDÓNIMO

Existem muitos serviços de correio eletrónico temporário que pode utilizar para se inscrever em sítios Web, para evitar ter de partilhar o seu nome e endereço de correio eletrónico verdadeiros. O problema é que alguns não permitem regressar à caixa de entrada mais tarde, quando é necessário recuperar informações importantes da conta. Os serviços gratuitos também tendem a estar cheios de localizadores, pelo que não são tão privados como seria de esperar.

Uma solução é criar pseudónimos de correio eletrónico utilizando o SimpleLogin (https://tinyurl.com/ywrvz6rn), que é desenvolvido pela empresa suíça de privacidade Proton. Utilize um pseudónimo para se registar num sítio ou serviço e o SimpleLogin reencaminhará todas as mensagens enviadas para o endereço de correio eletrónico falso para o seu endereço verdadeiro - sem revelar este último a spammers, burlões e bisbilhoteiros. Pode até responder a e-mails utilizando o seu pseudónimo, para manter o seu disfarce.

O plano gratuito do SimpleLogin permite-lhe criar até 10 pseudónimos, utilizando o seu prefixo e domínio preferidos ou gerando um aleatório. As suas extensões de browser e aplicações móveis permitem-lhe aceder aos seus pseudónimos em tempo real e desativá-los conforme necessário. O plano Premium do SimpleLogin (para o qual obtém uma

**Mantenha o seu email real privado, criando outro falso ou temporário com a ajuda do SimpleLogin**

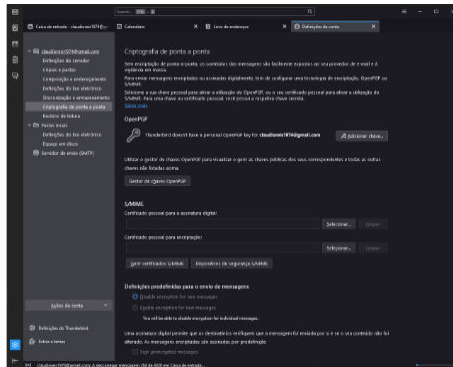
avaliação gratuita de sete dias) custa 30 dólares (aproximadamente 28 euros) por ano e inclui aliases e caixas de correio ilimitados, bem como domínios personalizados.

O DuckDuckGo inclui uma funcionalidade semelhante, a proteção de e-mail (https://tinyurl.com/vpts5fbt), nas suas aplicações móveis, no navegador para computador e nas extensões. Esta funcionalidade permite-lhe criar um número ilimitado de endereços "@duck.com", que reencaminham as mensagens para a sua conta de correio eletrónico real e removem os rastreadores incorporados. Está atualmente em fase beta, mas funciona muito bem.

## ENCRIPTAR OS SEUS E-MAILS PRIVADOS NO THUNDERBIRD

O ProtonMail (https://tinyurl.com/mt5wmp9z) e o Tuta (https://tinyurl.com/pym872yx) fornecem serviços de correio eletrónico encriptado gratuitos, mas limitam-no a 1 GB de armazenamento.

Para manter o seu endereço de correio eletrónico atual, proteger mensagens sensíveis e nunca ficar sem espaço, utilize as funcionalidades de encriptação do Mozilla Thunderbird (https://tinyurl.com/mpc7knmu).

Clique no botão de menu de três linhas no canto superior direito da janela principal do Thunderbird e selecione 'Definições da conta' e, em seguida, 'Criptografia de ponta a ponta'. Clique em 'Add Key' ('Adicionar chave'), selecione 'Create a new OpenPGP key' ('Criar uma nova chave OpenPGP') e clique em 'Continue' ('Continuar'). Escolha o seu endereço de correio eletrónico no menu 'Identity' ('Identidade'), especifique por quantos anos a sua chave deve funcionar e clique em 'Generate key' ('Gerar chave'). Clique em 'Confirm' (Confirmar) e o Thunderbird irá gerar a

**As ferramentas de encriptação integradas no Thunderbird mantêm os seus emails completamente privados**

sua chave OpenPGP - esta é composta por partes públicas e "secretas".

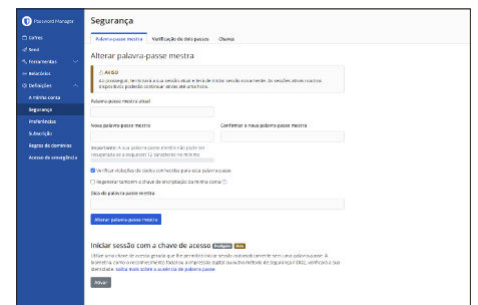
Para enviar uma mensagem encriptada a alguém, é necessário que essa pessoa lhe envie primeiro a sua chave de encriptação pública. Abra o e-mail que contém esta chave, faça duplo clique no anexo '.asc' e clique em 'Importar' para guardar a chave no Thunderbird. Quando redigir uma nova mensagem para essa pessoa, clique no botão 'Encriptar' e, em seguida, escreva e envie o seu e-mail. A sua chave de encriptação pública será automaticamente anexada, para que o destinatário - mas mais ninguém - possa desencriptar e ler a mensagem.

Para partilhar a sua chave pública com pessoas a quem não enviou mensagens privadas anteriormente, clique na seta junto a 'Anexar' e seleccione 'A minha chave pública PGP aberta'. Isto envia-lhes um anexo de correio eletrónico contendo a sua chave, para que eles possam responder com a sua chave e possam trocar mensagens encriptadas.

## PROTEJA AS SUAS CONTAS ONLINE UTILIZANDO CHAVES DE ACESSO

As chaves de acesso permitem-lhe iniciar sessão em sítios Web e aplicações utilizando a sua impressão digital, rosto ou um PIN de bloqueio de ecrã, da mesma forma que desbloqueia o seu PC ou telemóvel. Uma vez que estes dados são armazenados no seu dispositivo e não nos respectivos serviços, são mais seguros e mais convenientes do que as palavras-passe.

O nosso gestor de palavras-passe gratuito favorito, o Bitwarden (www.snipca.com/50153), suporta agora as chaves de acesso, para lhe proporcionar uma forma mais simples de proteger os seus dados privados. Instale a extensão Bitwarden (https://tinyurl.com/3mr2ekvc), inicie sessão na sua conta e visite um sítio que suporte chaves de acesso (consulte a lista em https://tinyurl.com/y6afh99x). Aceda à secção 'Segurança' das definições da sua conta, encontre a opção para configurar uma chave de acesso (Activar em 'Iniciar sessão com a chave de acesso) e escolha o seu método de início de sessão preferido - telefone, tablet, Windows Hello ou chave de segurança. O Bitwarden irá oferecer-se para guardar a nova chave de acesso - escreva Bitwarden quando lhe for perguntado onde. Da próxima vez que visitar o sítio, poderá iniciar sessão utilizando a chave de acesso em vez de uma palavra-passe.

O Bitwarden introduziu recentemente a opção de iniciar sessão no seu cofre Web com uma chave de acesso, em vez de uma palavra-passe mestra - clique em 'Ativar' em 'Iniciar sessão com chave de acesso' nas definições

**O Bitwarden permite agora que entre nas suas contas em websites usando chaves de acesso**

de Segurança. Também adicionou o suporte de passkey à versão beta da sua aplicação iOS (https://tinyurl.com/3b8pyyfx).

**Elimine todos os seus dados de navegação usando, por exemplo, a extensão Clear Browsing Data para o Chrome**

# APAGUE TODOS OS VESTÍGIOS DAS SUAS ACTIVIDADES NA WEB

## ELIMINE TODOS OS SEUS DADOS DE NAVEGAÇÃO COM UM CLIQUE

Uma das funcionalidades mais úteis do navegador do DuckDuckGo é o botão 'Fire', que fecha os separadores abertos e elimina os dados de navegação com um só clique. Isto inclui detalhes dos sítios que visitou; os seus cookies, caches e favicons; e quaisquer permissões que lhes tenha concedido (como a sua localização).

Poupa-lhe o incómodo de limpar estes elementos manualmente, mantém as suas atividades privadas e permite-lhe iniciar a sua próxima sessão de navegação com um quadro limpo.

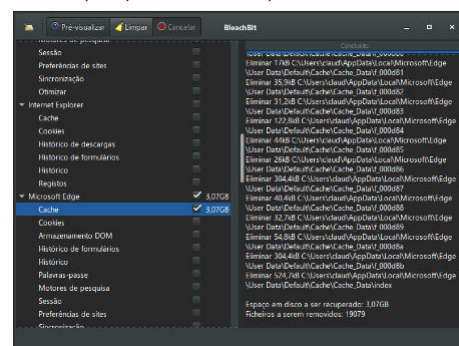
Pode adicionar uma função do tipo botão de disparo a outros browsers instalando Clear Browsing Data for Chromium (https://tinyurl.com/mskesaj8) e Firefox (https://tinyurl.com/282zvh5k). Esta extensão permite-lhe eliminar os cookies, a cache, os dados do formulário, o histórico e outros elementos clicando no botão da barra de ferramentas e escolhendo a opção relevante. Em alternativa, pode limpar todos os dados de navegação de uma só vez, selecionando 'All Data Types' ('Todos os tipos de dados').

Para especificar os tipos de dados a incluir, aceda às 'Options' ('Opções') da extensão e assinale/desmarque as caixas no menu do lado esquerdo. Pode replicar mais fielmente o botão Disparar do DuckDuckGo definindo 'Clear Browsing Data' ('Limpar dados de navegação') para eliminar todos os tipos de dados e fechar todos os separadores diretamente a partir do botão da barra de ferramentas - desactive a opção 'Ask before removing data' ('Perguntar antes de remover dados') para ignorar o pedido de confirmação.

## LIMPE OS DADOS DE TODOS OS SEUS NAVEGADORES DE UMA SÓ VEZ

Se alternar entre vários browsers no seu PC, é fácil esquecer quando e onde pode ter comprometido a sua privacidade - por exemplo, ao não sair de uma conta pessoal ou ao não apagar detalhes de pesquisas sensíveis. Em vez de abrir cada um dos browsers para aceder às respetivas definições e apagar os seus rastos, limpe tudo de uma só vez com o BleachBit (www.bleachbit.org).

Esta poderosa ferramenta de limpeza gratuita deteta automaticamente quais os navegadores instalados e lista todos os tipos de dados que pode apagar, incluindo cookies, caches, pesquisas, histórico de navegação e preferências de sites. Para obter opções adicionais e incluir navegadores que o BleachBit não identifica por predefinição (como o Vivaldi), clique no botão de menu no canto superior esquerdo, escolha 'Preferências' e selecione 'Descarregar e atualizar produtos de limpeza da comunidade'. Clique em 'Guardar' e verá uma lista alargada de definições do navegador, incluindo o misterioso 'armazenamento de blob' (dados não estruturados de serviços online).

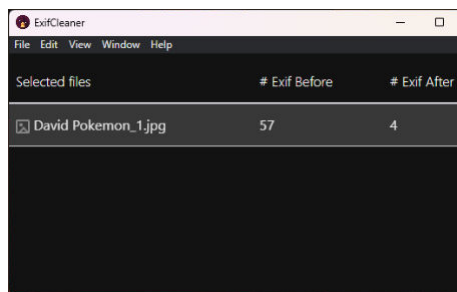
Assinale as caixas junto a todos os itens que pretende limpar - ou a caixa

**Faça desaparecer dados privados de todos os seus navegadores de uma só vez usando o BleachBit**

junto ao nome de um navegador para selecionar todos os seus dados - e clique no botão Pré-visualizar. O BleachBit irá então listar todos os elementos a serem removidos e indicar a quantidade de espaço em disco que irá recuperar - irá avisá-lo sobre a eliminação de itens importantes, tais como palavras-passe guardadas. Clique em 'Limpar' para limpar todos os seus navegadores de dados privados e ficheiros inúteis.

### REMOVER DADOS PRIVADOS DE FOTOGRAFIAS E VÍDEOS

As câmaras digitais e os smartphones registam informações sobre as fotografias que tira sob a forma de metadados EXIF. Estes são armazenados no ficheiro de imagem e incluem detalhes sobre quando e onde a fotografia foi tirada e o dispositivo utilizado.

Embora estes metadados sejam úteis para organizar as fotografias por data e local, também representam um risco para a privacidade quando partilha fotografias online. Os estranhos que estudarem os dados EXIF poderão identificar onde vive e onde esteve a partir das coordenadas GPS. Por este motivo, é aconselhável remover os dados de localização de determinadas imagens antes de as publicar nas redes sociais e noutros sites.

A melhor ferramenta gratuita para este fim é o ExifCleaner, que pode ser

**Use o ExifCleaner para remover os metadados de fotos e vídeos antes de os partilhar**

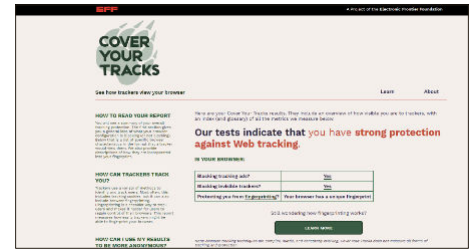
descarregado a partir de www.snipca.com/50164 - clique na ligação 'ExifCleaner-3.6.0.exe' em Assets. Basta arrastar e largar as imagens para a janela do programa, ou clicar em 'Open' ('Abrir') no menu 'File' ('Ficheiro') para as selecionar manualmente e o ExifCleaner removerá automaticamente os dados EXIF do ficheiro e mostrará as figuras "antes" e "depois".

O programa suporta todos os principais formatos de imagem, incluindo JPEG, PNG, BMP, GIF e TIFF, e também pode remover metadados de vídeos. Embora não tenha sido atualizado desde 2021, tem um atestado de boa saúde no VirusTotal (https://tinyurl.com/yywmmzvx).

Pode remover metadados de fotografias no seu dispositivo móvel utilizando aplicações gratuitas, como o Photo Metadata Remover para Android (https://tinyurl.com/p8ha9m8n) e o Exif Metadata para iOS (https://tinyurl.com/3nbr93sy).

## TESTAR A SUA PRIVACIDADE UTILIZANDO FERRAMENTAS ONLINE

### TESTE A PRIVACIDADE DO SEU NAVEGADOR WEB

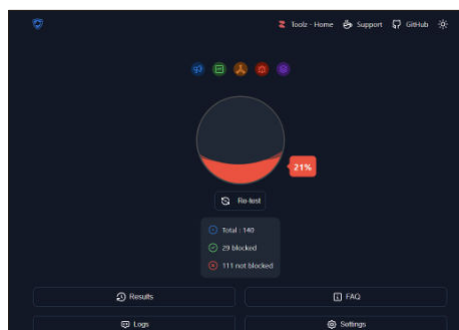
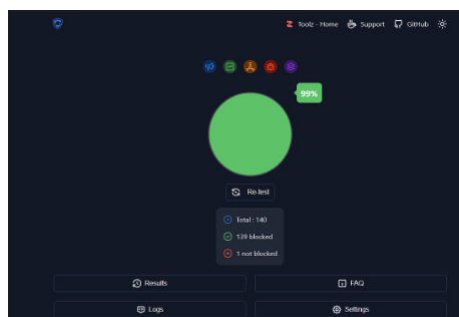
Não parta do princípio de que as definições de privacidade do seu navegador - especialmente a opção 'Não seguir', notoriamente ineficaz - impedirão os sítios Web de o identificar e seguir. Em vez disso, visite a ferramenta gratuita Cover Your Tracks (https://tinyurl.com/mtf4c82u) do grupo de defesa da privacidade Electronic

**O Cover Your Tracks testa a proteção do seu navegador contra rastreadores**

Frontier Foundation, selecione a caixa 'Test with a real tracking company' e clique em 'Test Your Browser'.

Dentro de alguns segundos, o site dir-lhe-á se o seu navegador está a bloquear anúncios de rastreio, rastreadores invisíveis e impressões digitais, e quantos bits de informação de identificação está a deixar escapar - desloque-se para a secção 'Detailed Results' (Resultados detalhados) para saber quais são.

Nos nossos testes, apenas o Navegador Tor e o Brave (com a sua impressão digital "agressiva" ativada) ofereceram proteção completa.

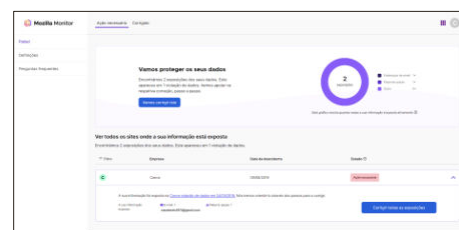
### CONFIRMAR SE O BLOQUEADOR DE ANÚNCIOS E A VPN ESTÃO A FUNCIONAR

Embora recomendemos o uBlock Origin como a melhor forma de bloquear anúncios e rastreadores, existem muitas alternativas boas - certifique-se apenas de que a ferramenta escolhida funciona como prometido. O Adblock Test (https://tinyurl.com/yd5kcpxf) testa a eficácia do seu bloqueador contra anúncios, scripts de rastreio, ferramentas de análise, rastreadores de redes sociais e outros elementos intrusivos e atribui-lhe uma pontuação percentual de proteção. Tente efetuar o teste com o bloqueador de anúncios ativado e desativado para comparar a diferença. No nosso teste, o uBlock Origin obteve 99% de proteção, bloqueando 139 de

**Teste o seu bloqueador de anúncios para se certificar que efetivamente bloqueia rastreadores**

140 elementos, mas sem ele o Chrome obteve apenas 21%, bloqueando apenas vinte e nove.

Da mesma forma, pode verificar se a sua VPN ou outra ferramenta de anonimato está a disfarçar o seu endereço IP visitando IPleak.net (https://ipleak.net). Se a sua localização real e o seu ISP forem apresentados na caixa 'IP address details', a sua privacidade não está a ser devidamente protegida.

### VERIFIQUE SE OS SEUS DADOS FORAM VIOLADOS

O Mozilla Monitor (https://tinyurl.com/bdckm8c8), anteriormente designado por Firefox Monitor, verifica o seu endereço de e-mail na base de dados Have I Been Pwned para determinar se esteve envolvido em alguma violação de dados. Em caso afirmativo, apresenta avisos de 'Action needed' (Ação necessária), diz-lhe quais as informações afetadas e permite-lhe clicar em 'Fix all exposures' (Corrigir todas as exposições) para obter conselhos sobre como proteger as suas contas. O Mozilla Monitor funciona em todos os browsers e está agora integrado com o gestor de palavras-passe do Firefox para o alertar quando os seus dados tiverem sido comprometidos. É necessária uma conta Mozilla para utilizar a ferramenta gratuita - um novo plano Plus pago, que remove as suas informações pessoais dos sítios de corretores de dados, está atualmente limitado aos EUA. ■

## É possível conversar em privado com ferramentas de Inteligência Artificial?

A ascensão dos chatbots de IA, como o ChatGPT e o Microsoft Copilot, deu origem a preocupações de privacidade sobre a forma como estas ferramentas recolhem os seus dados. Quaisquer perguntas e comandos que introduza são armazenados e partilhados para treinar os modelos de IA e melhorar a precisão das suas respostas, mas também estão ligados à sua identidade online - incluindo a sua localização, endereço de correio eletrónico e número de telefone.

No ano passado, a OpenAI, proprietária do ChatGPT, abordou as preocupações com a privacidade adicionando a opção de permitir que os utilizadores desliguem o 'Histórico e treino de conversação'. Esta opção encontra-se na secção 'Controlos de dados' ('Data controls' das definições da ferramenta no sítio Web do ChatGPT e na sua aplicação móvel, onde também pode limpar o seu histórico de conversações. Mas isto apenas impede que as suas conversas sejam utilizadas para fins de formação - a OpenAI continuará a armazená-las durante 30 dias e a associá-las a si.

O novo chatbot Leo da Brave (https://tinyurl.com/25c6xbz8) é mais fiável, porque não requer uma conta, não recolhe informações como o seu endereço IP nem armazena as suas conversas. Também pode experimentar a aplicação para Android 'Chat with AI - Incognito' (https://tinyurl.com/58kpd5jx), que afirma fornecer "anonimato completo", não exigindo uma conta, armazenando os seus dados ou permitindo que terceiros o localizem.

# Desista do Google. Use o ChatGPT!

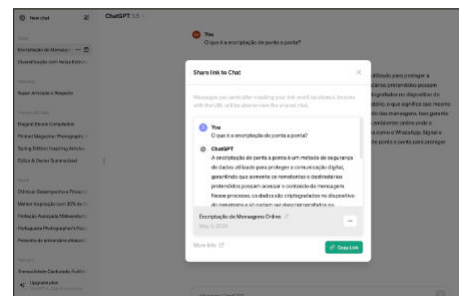
**A poderosa ferramenta de Inteligência Artificial (IA) ChatGPT dá-lhe frequentemente respostas mais detalhadas do que o Google - e sem anúncios. Explicamos como a utilizar.**

Pela primeira vez em quase 25 anos, o Google está preocupado com a possibilidade de ser destronado como a principal ferramenta de pesquisa do mundo. A razão é a sensacional ascensão do ChatGPT. Lançado no final de 2022, é uma ferramenta de IA que responde a perguntas dactilografadas em inglês simples (e também em português e outros idiomas), normalmente em apenas alguns segundos. É uma das poucas ferramentas de IA que justificam o aumento do hype em torno da tecnologia.

A utilização do ChatGPT tornou-se mais fácil desde o início de abril, quando o OpenAI - o organismo de investigação que gere a ferramenta - a abriu para ser utilizada sem necessidade de registo de uma conta. Tudo o que precisa de fazer é visitar https://chat.openai.com e começar a escrever na caixa 'Message ChatGPT' na parte inferior. Quando terminar, clique no botão "Send message" (seta a apontar para cima) ou prima Enter. Tenha em atenção que isto está a ser implementado para utilizadores de todo o mundo, pelo que, por enquanto, pode ainda ser necessário iniciar sessão.

A OpenAI não é uma instituição de caridade e sabe que há muito dinheiro a ganhar com o ChatGPT. Por isso, cobra a partir de 20 dólares por mês pela versão 'Plus', que lhe dá resultados mais precisos, tecnologia de IA mais recente, a possibilidade de guardar as suas conversas e outras funcionalidades como plug-ins. Mas, de acordo com a nossa experiência, a edição gratuita é suficientemente boa para a maioria das pessoas.

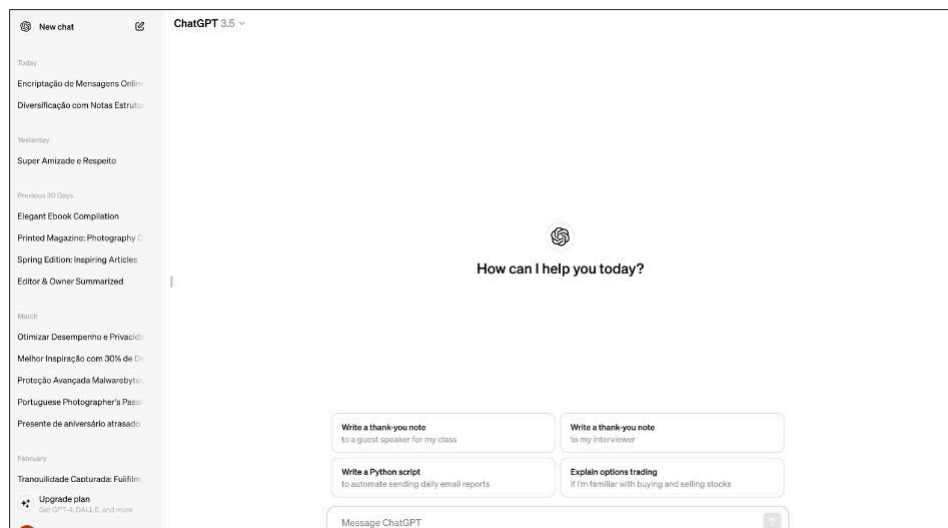
Também é fácil partilhar resultados com outras pessoas. Clique no ícone 'Share link to Chat' no canto superior direito e, em seguida, copiar e colar a ligação numa aplicação de mensagens ou num e-mail. Por predefinição, os chats são partilhados de forma anónima. Para adicionar o seu nome, clique nos três pontos e selecione 'Share your name'.

A maior desvantagem do ChatGPT gratuito é que se baseia em informações que foram atualizadas pela última vez em janeiro de 2022. Isto significa que não deve utilizá-lo para obter previsões meteorológicas, atualizações de notícias ou os últimos

**Pode facilmente partilhar os resultados com outras pessoas, bastando clicar no ícone no canto superior direito, 'Share link to Chat'**

conselhos de compra. Mas é melhor do que o Google em muitos outros aspetos, como explicaremos.

## DEFINIÇÕES DE JARGÃO TECNOLÓGICO

Perguntámos ao ChatGPT "O que é a encriptação de ponta a ponta?" e ele deu-nos uma resposta que atingiu o equilíbrio perfeito entre brevidade e detalhe: "A encriptação de ponta a ponta é um método de segurança de dados utilizado para proteger a comunicação digital, garantindo que somente os remetentes e destinatários pretendidos possam aceder ao conteúdo da mensagem. Nesse processo, os dados são criptografados no dispositivo do remetente e só podem ser descriptografados no dispositivo do destinatário, o que significa que mesmo os provedores de serviços de comunicação não têm acesso ao conteúdo das mensagens. Isso garante uma camada adicional de privacidade e segurança, especialmente em ambientes online onde a interceptação de dados é uma preocupação. Aplicações de mensagens como o WhatsApp, Signal e Telegram são exemplos de plataformas que empregam a encriptação de ponta a ponta para proteger as comunicações dos utilizadores.".

Descobrimos que é igualmente preciso ao definir outros tipos de jargão

**Depois de entrar no ChatGPT, pergunte ou ordene que que quer que o assistente de Inteligência Artificial responda ou faça por si, na caixa 'Message ChatGPT. Depois clique na seta para cima, ou prima Enter**

tecnológico. Perguntar ao Google sobre encriptação de ponta a ponta traz páginas de ligações, mas não há forma de saber qual é a mais fácil de compreender. Pode clicar nas opções 'As pessoas perguntam frequentemente' para obter mais informações, mas estas são menos detalhadas do que as respostas do ChatGPT.

## NEWSLETTERS E CONVITES PARA EVENTOS

O ChatGPT satisfez sem esforço o nosso pedido de um modelo de newsletter para convidar os membros de um clube para uma Assembleia Geral Anual. Gostámos do resultado, mas pedimos uma versão mais amigável e o ChatGPT tornou instantaneamente o texto mais conversador e menos formal. Isto demonstra um dos pontos fortes do ChatGPT: pode responder a pedidos de seguimento com respostas alteradas. É realmente como entrar numa conversa e é mais natural do que os chatbots medíocres com que muitas vezes temos de lidar online. Isto revela-se especialmente útil quando não compreende a resposta original, porque pode pedir-lhe uma resposta mais simples.

Ao perguntar por um modelo de boletim informativo no Google, surgem novamente muitos links que podem ser úteis, mas terá de adivinhar qual é o mais adequado para si.

## MODELOS DE CARTAS SOBRE OS DIREITOS DOS CONSUMIDORES

Saber como apresentar uma queixa eficaz é fundamental para obter os resultados que pretende quando lida com empresas. Terá mais hipóteses se utilizar um modelo de carta que contenha a redação correta e as informações legais. O Google tem links para vários sites que oferecem modelos, mas o ChatGPT pode escrevê-los por si - e ajustar as palavras para fins específicos.

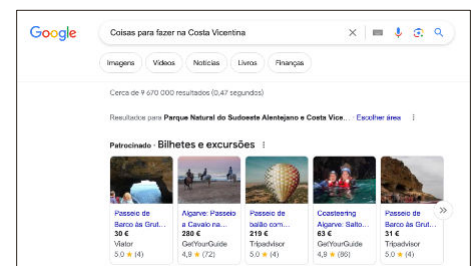
Pedimos-lhe que escrevesse uma carta para o serviço de apoio ao cliente da Amazon descrevendo o nosso direito de devolver um artigo defeituoso. O resultado foi um pouco vago, por isso pedimos-lhe que reescrevesse e mencionasse a Lei dos Direitos do Consumidor e os Regulamentos de Vendas à Distância. A carta foi enviada, indicando corretamente os direitos que lhe são conferidos.

## PLANOS DE FÉRIAS

O Google ganha a maior parte do seu dinheiro com anúncios online, por isso não é de admirar que a pesquisa por "Coisas para fazer na Costa Vicentina" produza uma fila de anúncios que se espalha pelo ecrã quando se clica neles. Tem um aspeto horrível.

Fazer a mesma pergunta ao ChatGPT deu-nos 8 sugestões previsíveis - praias, aldeias, passeios de barco, etc. Mais uma vez, a sua força reside na

## Em que é que o ChatGPT difere do Google

É importante lembrar que o ChatGPT não é um motor de busca. Quando lhe pergunta algo, não está a utilizar algoritmos para apresentar ligações a sítios Web com base nas palavras-chave que escreveu. Por conseguinte, não é possível utilizá-lo para encontrar o URL de um sítio Web. No entanto, tem vindo a recolher informações de toda a Internet para tornar as suas respostas relevantes. Ele utiliza essas informações ao analisar a sua pergunta, tentando fazer com que a resposta pareça humana.

**Pergunte qualquer coisa ao Google sobre o que fazer em férias e verá o ecrã invadido por publicidades**

**Depois de termos pedido ao ChatGPT para criar um modelo de newsletter para convidar membros de um clube, não satisfeitos solicitamos uma versão mais amigável, o que feito sem qualquer tipo de reclamação**

**Férias com a ajuda do ChatGPT são um descanso. Depois de nos indicar o que fazer na Costa Vicentina, pedimos para que nos especificasse quais as melhores praias acessíveis a pessoas em cadeiras de rodas, o que ele fez com prontidão**

resposta a pedidos de mais pormenores.

Pedimos-lhe para ser mais específico em relação às praias, depois para excluir as que são difíceis para pessoas em cadeiras de rodas. Por fim, pedimos-lhe que sugerisse os melhores bares perto dessas praias. O ChatGPT deu respostas cada vez mais específicas. O ChatGPT também fornece itinerários pormenorizados para viagens que envolvem diferentes destinos e períodos.

## INSTRUÇÕES DE COMO FAZER

As pesquisas "Como fazer" são tão populares no Google que, normalmente, são incluídas no top 10 anual dos resultados "em tendência". Verá links para sites e vídeos com instruções, mas é mais rápido utilizar o ChatGPT. Escrevemos "Como sangrar um radiador" e o ChatGPT explicou o processo em 8 passos, juntamente com os materiais necessários e as precauções de segurança. Acrescentou mais detalhes quando o pedimos e destacou o que poderia correr mal.

O ChatGPT não fornece instruções em vídeo, pelo que, dependendo da complexidade da tarefa, poderá ter de visitar o YouTube para obter orientação. Mas continua a ser o ponto de partida perfeito quando precisa de conselhos para tarefas práticas.

## PERGUNTAS DE QUIZ

Este é outro exemplo em que o Google sugere páginas de sites, enquanto o ChatGPT lhe dá resultados diretos. Pedimos-lhe perguntas sobre filmes, história, geografia, astronomia e literatura, que tornámos mais específicas ao restringir a categoria - por exemplo, filmes vencedores de Óscares nos anos 50 e Guerras das Rosas. Pedimos que as perguntas fossem mais difíceis ou mais fáceis até atingirmos o equilíbrio correto.

## ESCREVER HISTÓRIAS E POEMAS

Embora o ChatGPT ofereça ajuda prática, também sabe como se divertir. Peça-lhe para escrever uma história ou um poema e ele criará algo relevante, divertido e muitas vezes surrealista. É capaz de lidar com muitos pormenores, incluindo o assunto, o local, os temas e o estilo. Por exemplo, pedimos-lhe para escrever "um thriller de espionagem sobre um texugo paranoico chamado João, ao estilo de John le Carré, passado em Berlim". Produziu três capítulos, depois mais dois quando lhe pedimos, antes de nos dar um final trágico quando lho pedimos.

**Até histórias este modelo de Inteligência Artificial pode escrever por ou para si**

Estas histórias não vão substituir os verdadeiros escritores - pelo menos, esperamos que não - mas é espantoso ver o ChatGPT criar trabalho a partir dos seus comandos. É também fascinante ver até onde se pode ir com a sua criatividade com comandos cada vez mais obscuros e específicos. ■

## 5 coisas que o ChatGPT não faz

**1.** Dar conselhos criminais, por exemplo, como mentir à polícia ou ocultar provas. Também não responderá a perguntas sobre o consumo de drogas.

**2.** Revelar informações sobre outras pessoas que invadam a sua privacidade.

**3.** Fazer previsões sobre o futuro, tais como previsões financeiras ou sobre quem vai ganhar jogos desportivos.

**4.** Envolver-se em "discursos de ódio" ou promover qualquer forma de conteúdo prejudicial.

**5.** Dar a sua opinião sobre questões como cultura, política, entretenimento, problemas sociais e outros.

# Faça o derradeiro exame ao estado de saúde do seu computador

**Saiba mais sobre o funcionamento interno do seu PC e detete falhas de hardware efetuando uma auditoria ao sistema com o Glow. Neste artigo, revelamos o que verificar com este brilhante programa gratuito.**

**Obtenha informação valiosa sobre o seu PC no separador 'Operating System' do Glow**

É sempre útil saber o que se passa no interior do seu PC, mas o software de informação do sistema é muitas vezes confuso (como o CPU-Z), pago (como o SIW) ou desatualizado (como o Speccy). O Glow (https://tinyurl.com/kz5z8jr5) fornece uma forma simples, gratuita e moderna de analisar o seu computador e acaba de lançar a sua terceira e última versão. Permite-lhe verificar se todo o seu hardware e software está a funcionar corretamente - permitindo-lhe detetar sinais precoces de falha - e obter muitas informações úteis.

Para descarregar o Glow, visite a sua página de versões (www.snipca.com/49138), clique na ligação 'Glow_v24.05.zip' e extraia o conteúdo do ficheiro ZIP. Faça duplo clique no ficheiro 'Glow_x64.exe' (se estiver a executar o Windows de 64 bits) ou 'Glow_arm64.exe' (se tiver um processador ARM) para executar o programa.

Uma vez que o Windows o considera como uma 'aplicação não reconhecida', o Glow irá disparar um aviso de segurança do Microsoft SmartScreen Defender, mas é completamente seguro de utilizar, por isso basta clicar em 'Mais informação' e depois em 'Executar mesmo assim'.

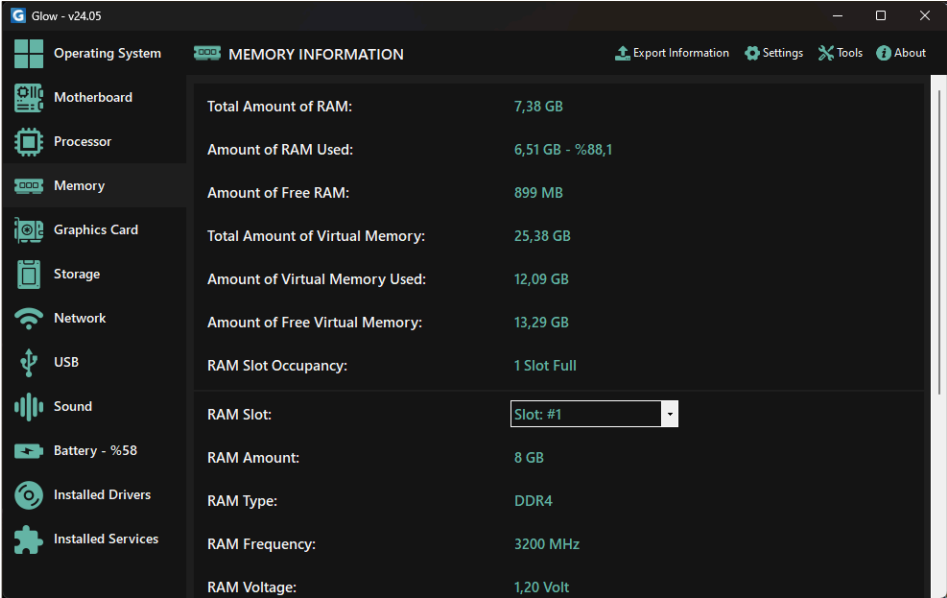
## VERIFIQUE AS ESPECIFICAÇÕES DO SEU SISTEMA

O separador 'Operating System' (Sistema Operativo) do Glow, que serve de ecrã inicial, fornece um resumo prático das especificações do seu PC. Estas incluem o fabricante e o modelo; a versão e a compilação do Windows que está a executar; e o endereço de e-mail da sua conta de utilizador registada.

O Glow também lista a ID do dispositivo, que é o número único do computador, e a ID do produto, que é o número associado à instalação do Windows. Este número é diferente da chave de licença que utilizou para ativar o sistema operativo e é utilizado principalmente para suporte técnico e resolução de problemas.

Percorra o separador 'Sistema Operativo' e encontrará informações interessantes sobre a última vez que o seu PC foi desligado e reiniciado, incluindo o "tempo de atividade" da sessão atual. Também pode verificar se o seu software antivírus e de firewall está a funcionar e ver quando foi a última vez que o seu computador sofreu o temido ecrã azul da morte.

## AUDITAR OS COMPONENTES DO SEU PC

Se está a pensar em atualizar o seu PC,

**O Glow informa a quantidade de memória atualmente disponível no seu PC**

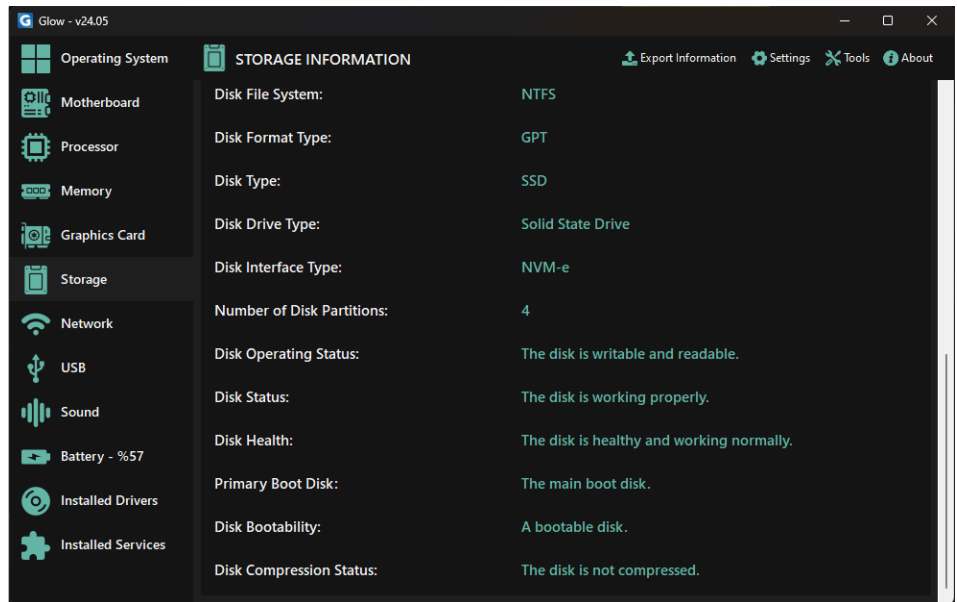
o Glow pode ajudá-lo a garantir que compra os componentes certos. Fornece dados completos sobre a placa-mãe, o processador e a memória, que normalmente teriam de ser encontrados no Windows. Pode saber o fabricante e o modelo destes componentes; verificar se o TPM 2.0 está ativado (essencial para instalar o Windows 11); e verificar a velocidade e o número de núcleos da sua CPU.

Particularmente útil é o separador 'Memory' (Memória), que revela a quantidade total de RAM instalada no seu sistema e a quantidade que está atualmente a ser utilizada - os mesmos detalhes são fornecidos para a memória virtual. O Glow até indica o tipo de RAM, como DDR4, e em que ranhuras os módulos estão inseridos.

Também vale a pena verificar o separador 'Graphics Card' (Placa Gráfica) para ver o modelo da sua GPU, confirmar se a placa gráfica está a funcionar corretamente e ver quando foi atualizado o controlador - se tiver sido há algum tempo, deve atualizá-lo manualmente. O mesmo separador indica a resolução do ecrã e a taxa de atualização do monitor.

## VERIFIQUE O ESTADO DO SEU DISCO RÍGIDO

O separador 'Storage' (Armazenamento) do Glow é muito mais informativo do que a secção com o mesmo nome na aplicação 'Definições' do Windows e diz-lhe tudo o que precisa de saber sobre os seus discos rígidos. Descubra o tamanho exato de cada unidade; o espaço disponível; o número de partições; o fabricante, modelo e número de série; o sistema de ficheiros - NTFS ou FAT32 - e até a interface, como SATA.

O melhor de tudo é que o Glow mostra rapidamente se a unidade está a funcionar corretamente, se é capaz de ler e escrever dados e se é

**Verifique a saúde do seu disco rígido e SSD no separador 'Storage'**

considerada saudável, o que significa que não está a abrandar ou a sofrer de sectores defeituosos (blocos de armazenamento inutilizáveis). Se tiver mais do que uma unidade, como um disco rígido mecânico e um SSD, alterne entre elas utilizando o menu pendente 'Disk Name' (Nome do disco) para atualizar as informações do Glow em conformidade.

## VER INFORMAÇÕES SOBRE OS SEUS ADAPTADORES

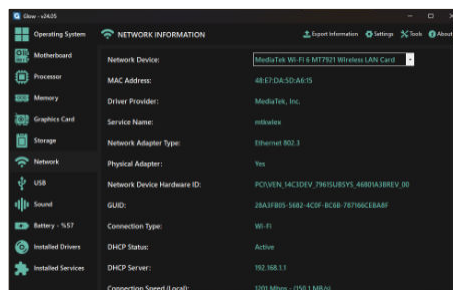
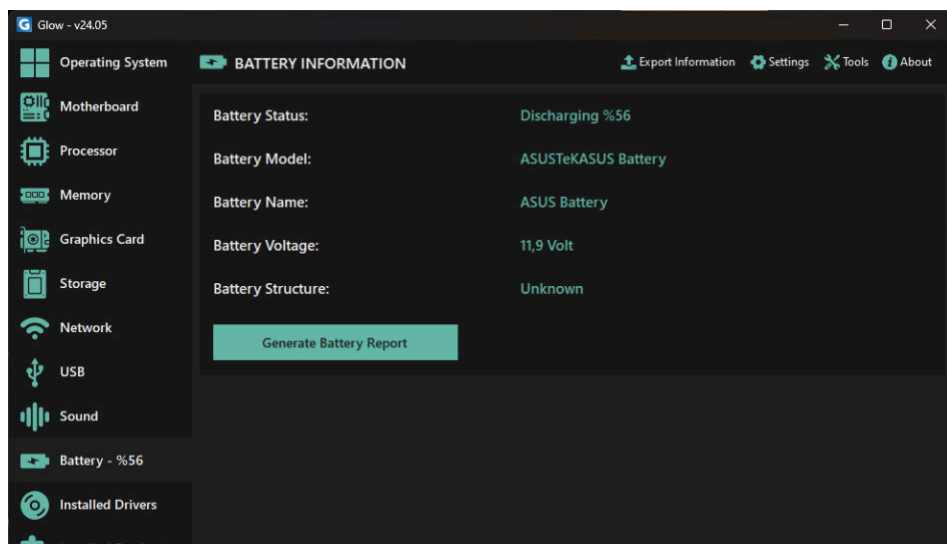
Os três separadores seguintes do Glow fornecem informações sobre os seus adaptadores de rede ('Network'), controladores USB ('USB') e placa de som ('Sound'). Por exemplo, no separador 'Network' (Rede), pode alternar entre os diferentes adaptadores instalados no seu PC para ver o tipo de ligação (Ethernet ou Wi-

Fi), o endereço MAC (o endereço físico único do dispositivo) e o endereço IP, que é utilizado para identificar a ligação de rede do adaptador. O Glow também apresenta a velocidade da ligação local, embora esta pareça ser um valor "até" para o adaptador e não uma medição em tempo real.

O separador 'USB' é útil principalmente para verificar se os seus dispositivos USB estão a funcionar corretamente, enquanto o separador 'Sound' (Som) faz o mesmo para os dispositivos de áudio e também indica os seus fabricantes e IDs de hardware.

## GERAR UM RELATÓRIO DA BATERIA DO COMPUTADOR PORTÁTIL

Pode utilizar o separador 'Battery' (Bateria) do Glow para avaliar o estado atual da bateria do seu computador portátil. Clique no botão 'Generate Battery Report' (Gerar relatório da bateria) para criar um relatório HTML e, em seguida, clique em 'Sim' para o abrir no seu navegador (o ficheiro também é guardado na pasta de instalação do Glow).

Descubra se a bateria do seu portátil está a perder capacidade solicitando ym relatório ao Glow

A secção 'Installed batteries' (Baterias instaladas) do relatório indica a capacidade da bateria do computador portátil, ou seja, a quantidade de energia que é capaz de armazenar (em mWh - miliwatts-hora), e a sua capacidade de carga total, ou seja, a quantidade de energia que contém quando está totalmente carregada. Se o segundo valor for muito inferior ao primeiro, poderá ser necessário atualizar o seu computador portátil.

O relatório também revela a contagem de ciclos do portátil - o número de vezes que a capacidade total da bateria foi esgotada. A maioria das baterias dura pelo menos 500 ciclos.

Abaixo desta informação, encontrará o seu histórico de utilização, que fornece uma análise semanal de quanto tempo o seu computador portátil funcionou com bateria e rede eléctrica, e o efeito que isso teve na capacidade e vida útil da bateria. Estes dados podem ajudá-lo a identificar o início dos problemas de desempenho.

**DETETAR CONTROLADORES DE DISPOSITIVO COM DEFEITO**

Para ver uma lista de controladores de dispositivos no Windows, é necessário abrir a 'Linha de Comandos', escrever 'driverquery' e tentar perceber o resultado. O Glow torna as coisas muito mais fáceis ao fornecer uma lista instantânea de todos os controladores instalados quando se clica no separador com esse nome.

Isto inclui o nome e o tipo de cada controlador e - ao contrário da lista da linha de comandos - se está a funcionar ou se parou. Opcionalmente, pode mostrar o caminho do ficheiro de cada controlador.

O separador 'Installed Services' (Serviços Instalados) oferece informações semelhantes para os processos em segundo plano do Windows, permitindo-lhe detetar atividades suspeitas e reativar serviços legítimos que tenham parado. O Glow não lhe permite alterar o estado ativo dos serviços ou controladores, mas é muito útil para referência. ■

## Melhore o seu PC utilizando as ferramentas avançadas do Glow

Embora o Glow seja principalmente um programa de informação do sistema, também inclui opções para otimizar o seu PC, que encontrará no menu 'Tools' (Ferramentas) no canto superior direito. Eis o que pode fazer com essas ferramentas.

**Ferramenta de automatização SFC & DISM**
Esta ferramenta deteta e repara ficheiros de sistema corrompidos utilizando as funcionalidades Verificador de Ficheiros de Sistema e Manutenção e Gestão de Imagens de Implementação do Windows (normalmente acessíveis através da Linha de Comandos). Prima Ctrl+Q para abrir a ferramenta e, em seguida, clique em 'Iniciar Reparação'.

**Ferramenta de limpeza de cache**
Liberte espaço no seu disco rígido eliminando ficheiros temporários e redundantes. O Glow oferece botões de limpeza com um clique para pastas como a Cache Temporária de Aplicações do Windows e o Histórico de Transferências do Windows Update. Prima Ctrl+W para iniciar esta ferramenta.

**UNINSTALR 2.4**

# Remova programas fácil e eficientemente

https://tinyurl.com/5duvrf8y

Quando escrevemos sobre o Uninstalr numa das últimas edições, ficámos surpreendidos com a sua ousada afirmação de ser o "melhor desinstalador do Windows". O programador até compilou uma tabela de comparação e um longo vídeo (www.snipca.com/50051) para provar a superioridade da nova ferramenta em relação a rivais estabelecidos, como o BCUninstaller e o HiBit Uninstaller.

Como salientámos, esta afirmação foi prejudicada pelo desempenho lento do Uninstair, por isso estamos satisfeitos por a versão 2.4 implementar muitas melhorias e correções. Embora ainda demore vários minutos a concluir a verificação inicial do software instalado, agora é mais rápido na remoção e faz um trabalho particularmente bom na deteção de restos que outras ferramentas não detetam.

O Uninstalr facilita a desinstalação em lote de vários programas de uma só vez, sem a necessidade de confirmar cada um deles. Em vez disso, basta selecionar as entradas na sua lista combinada de software, aplicações da Microsoft Store e possíveis resíduos e, em seguida, clicar no botão 'Desinstalar' (Unistall) para iniciar o processo de remoção. Isto dir-lhe-á quanto espaço poupará ao desinstalar os itens selecionados, juntamente com as pastas e chaves de registo relacionadas.

Para evitar interromper o seu trabalho, deve desmarcar as caixas para fechar todos os programas em execução antes da desinstalação e para reiniciar o seu PC depois, embora isto possa reduzir a sua eficácia. Clique em 'Iniciar Desinstalação' (Start Unistallation) e depois em 'Sim' (Yes) para confirmar. O Uninstalr não guarda cópias de segurança - embora crie pontos de restauro do sistema - pelo que deve rever cuidadosamente a lista de dados a remover.

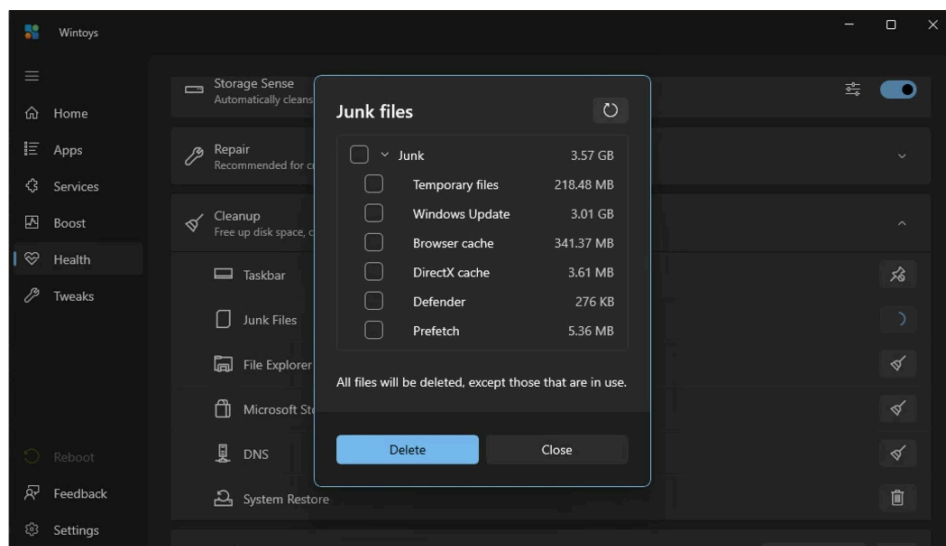
O programa atualizado deteta com precisão ferramentas antivírus e de segurança e avisa-o sobre a desinstalação das mesmas, e diz-lhe se o OneDrive está a sincronizar dados em segundo plano, o que pode levar a que uma aplicação removida seja restaurada. Também permite selecionar software de acordo com o seu tipo e editor.

O Uninstalr não é perfeito - continua a ser um pouco lento, demora demasiado tempo a atualizar as estatísticas e está sempre a sugerir que reinicie o computador. Mas é impressionantemente minucioso na remoção de lixo e poderá em breve justificar as afirmações do seu criador.

### WINTOYS 1.3

## Personalize e otimize o sistema operativo

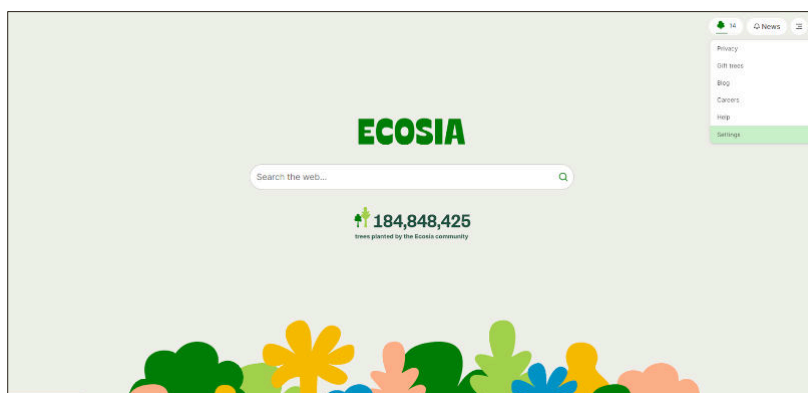
https://tinyurl.com/bdy39usd

Disponível na Microsoft Store, esta excelente aplicação gratuita oferece muitas formas de personalizar e otimizar o Windows - e esta atualização acrescenta ainda mais. Uma nova opção no separador 'Saúde' (Health) denominada “Pílula do sono” (Sleeping pill) impede que as tarefas agendadas, como as verificações em segundo plano, despertem o PC do modo de suspensão. Também no separador 'Saúde', uma nova ferramenta de “Diagnóstico de memória” (Memory diagnostics) verifica se o sistema tem problemas de memória - pode definir esta ferramenta para ser executada quando o PC for iniciado ou reiniciar e verificar imediatamente. O Wintoys melhorou o seu Limpador de Lixo (Junk cleaner), que se encontra na secção 'Limpeza' (Cleanup) do separador Saúde (Health), para incluir relatórios de erros e ficheiros de despejo na sua

lista de itens a remover, e adicionou a capacidade de limpar as caches de navegadores. Agora instala automaticamente as atualizações para que tenha sempre a versão mais recente da aplicação.

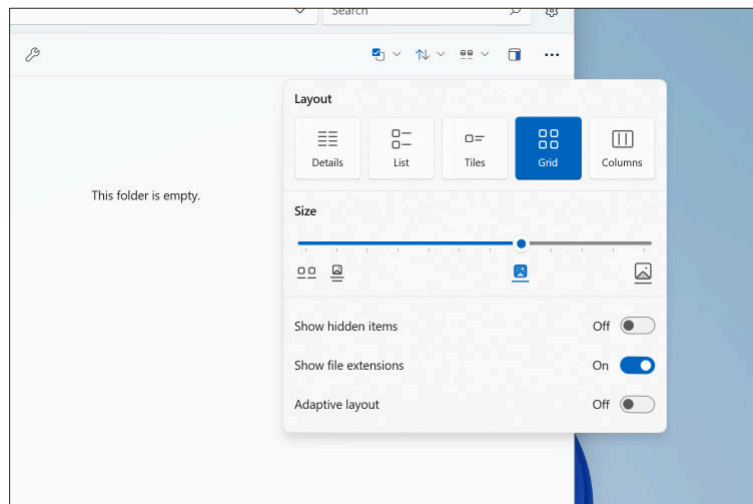
### ECOSIA BROWSER

## Navegador da Internet amigo do ambiente

https://tinyurl.com/4hj8crar

Ecosia, o motor de busca que doa o dinheiro que obtém com publicidade para projetos de plantação de árvores e outras iniciativas de ação climática, lançou aquilo que descreve como "o navegador mais verde da Terra". Baseia-se no código Chromium, portanto, assemelha-se muito ao Chrome, e protege a sua privacidade ao bloquear anúncios, rastreadores e pop-ups de consentimento de cookies - "menos anúncios também significam que está a consumir menos dados e energia". Pode personalizar o fundo da página inicial/nova página de separador utilizando fotos inspiradas nos projetos da Ecosia e monitorizar quantas árvores plantou (mais de 205 milhões no momento da escrita) e quanto dinheiro doou para a ação climática. Agora também tem um chatbot de IA.

FILES 3.3

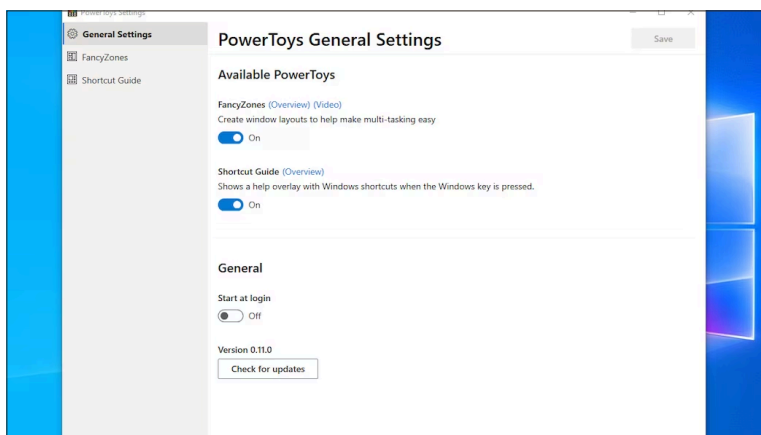
# Modifique a forma como vê e trata os ficheiros e pastas

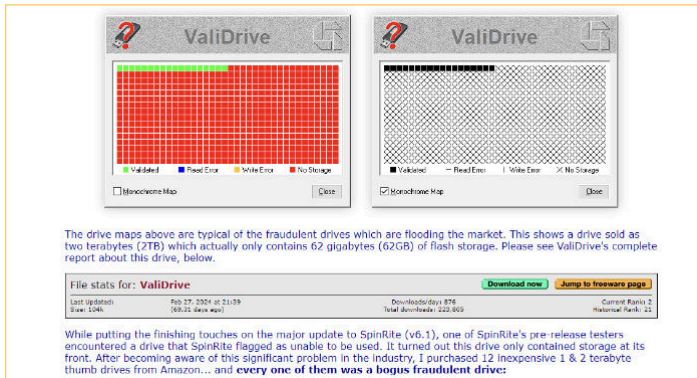
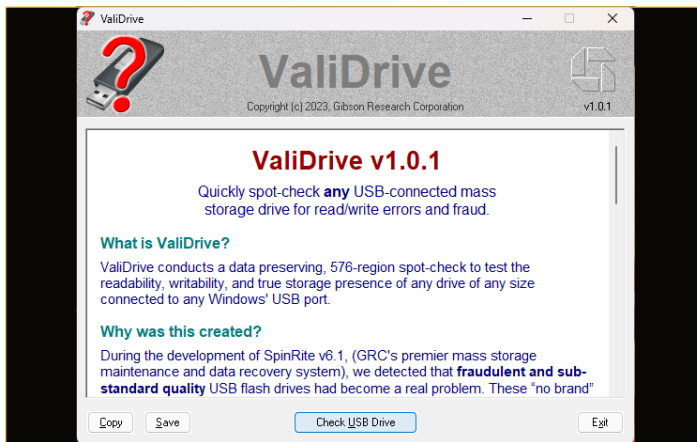
https://tinyurl.com/dpdkmxt2

A mais recente atualização desta brilhante alternativa ao Explorador de Ficheiros centra-se na melhoria do design do programa. As opções de 'Layout' no canto superior direito da janela principal do Files são agora apresentadas como uma fila de grandes azulejos. Isso facilita a troca entre os layouts 'Detalhes', 'Lista', 'Azulejos', 'Grelha' e 'Colunas' (Details, List, Tiles, Grid e Columns), dependendo do número e tipo de itens por que está a navegar. Agora pode ajustar o tamanho dos ficheiros e pastas usando o controlo deslizante de Tamanho, o que é útil para aumentar as miniaturas de imagens e vídeos.
Para alterar o layout predefinido para visualizar pastas, clique na engrenagem 'Configurações' (Settings) e abra a nova página de configurações de Layout. Aqui, pode escolher o seu tipo de layout preferido e como os itens devem ser ordenados - por nome, data ou tamanho. Como sempre com o Files, clique no link "instalador clássico" na página de download para obter a versão gratuita.

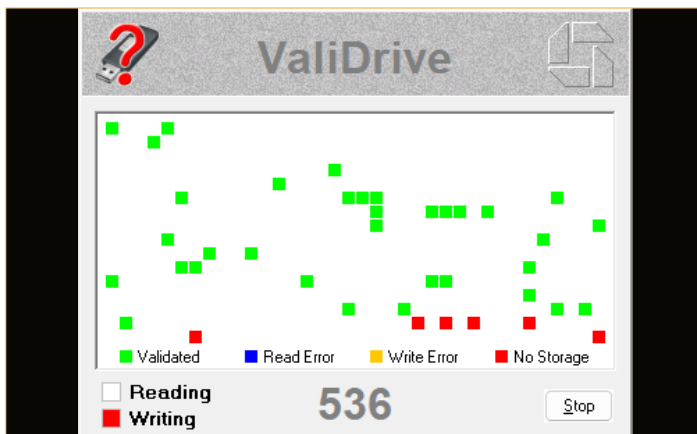
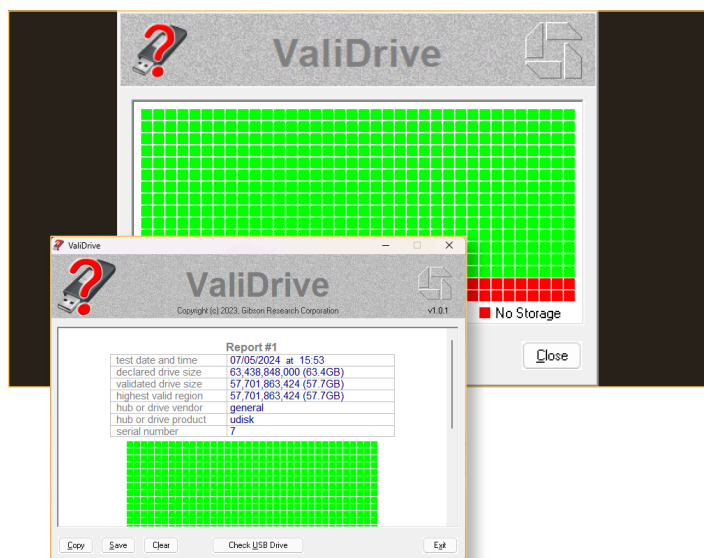
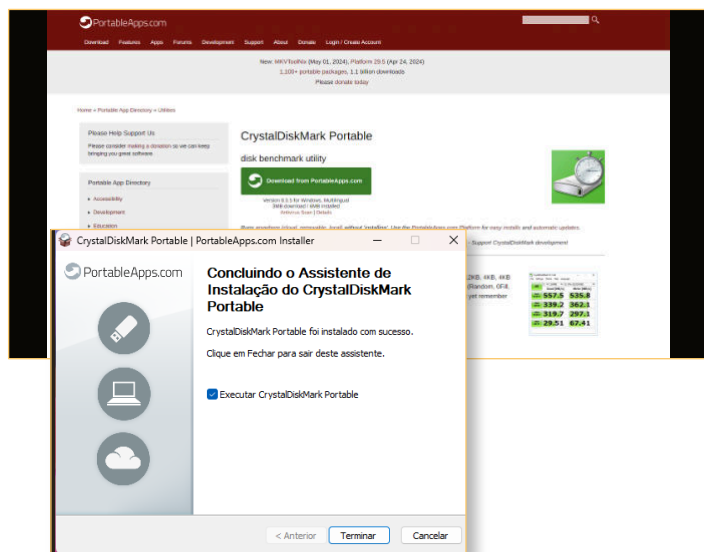
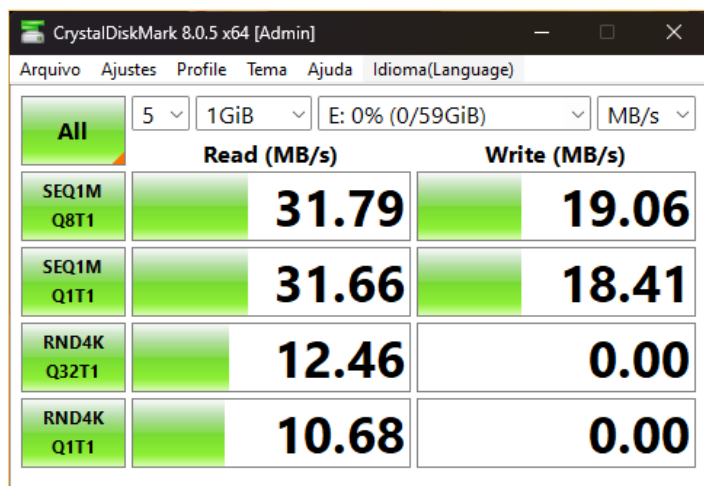
MICROSOFT POWERTOYS 0.80

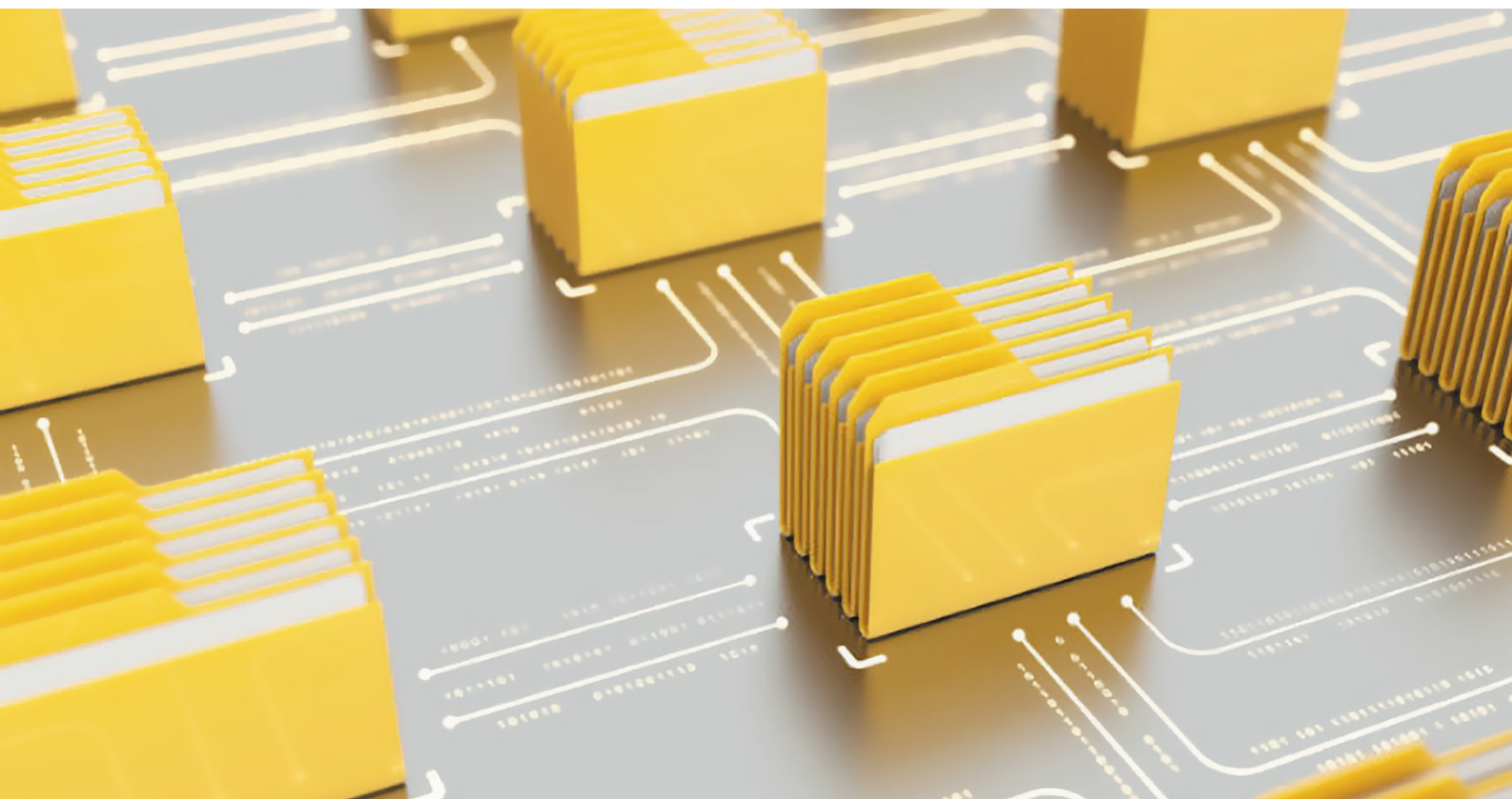
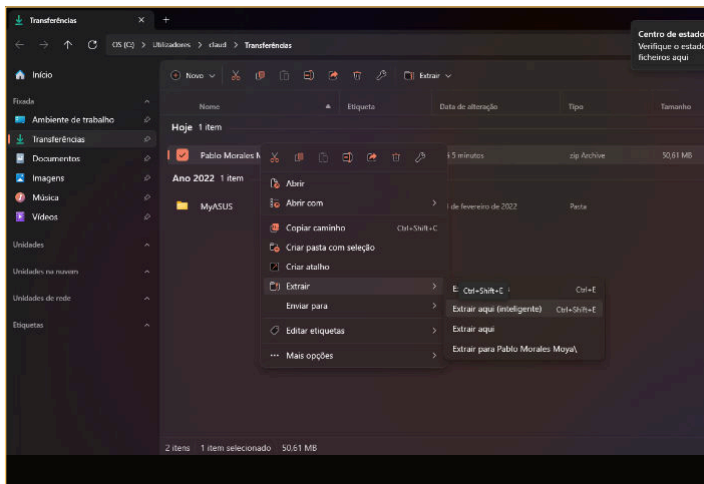
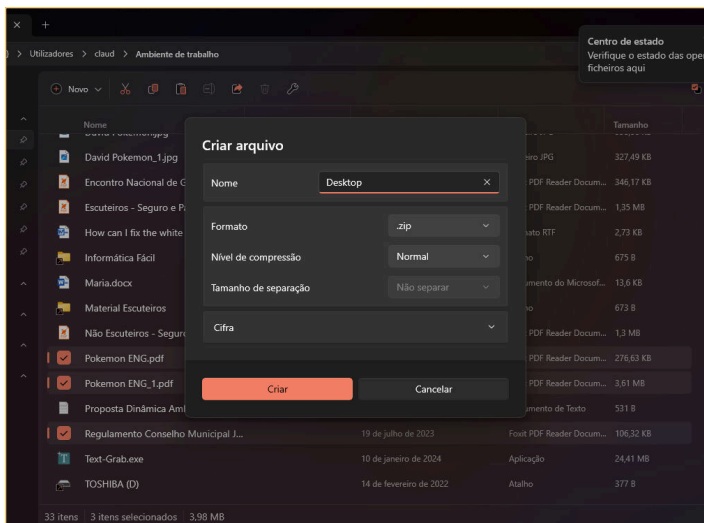
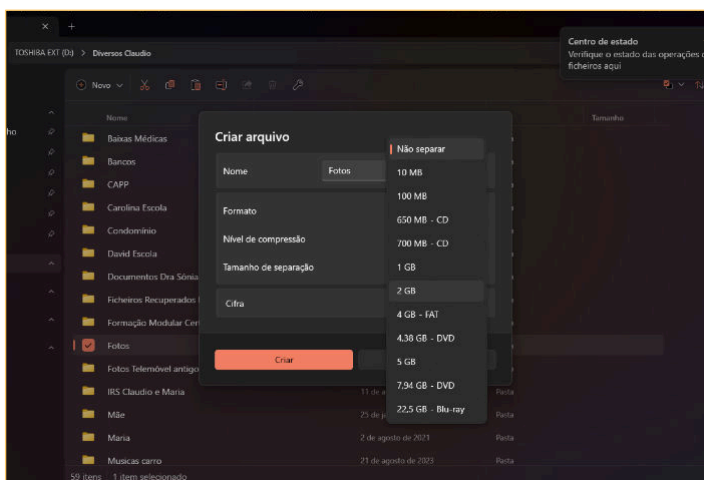
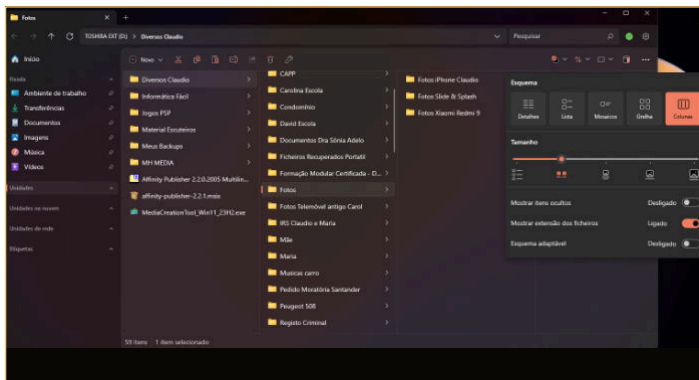
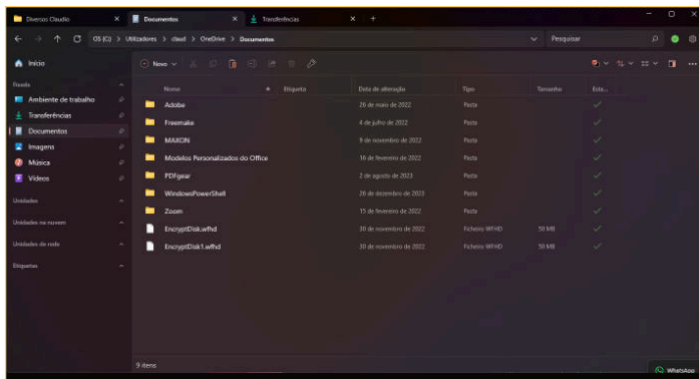
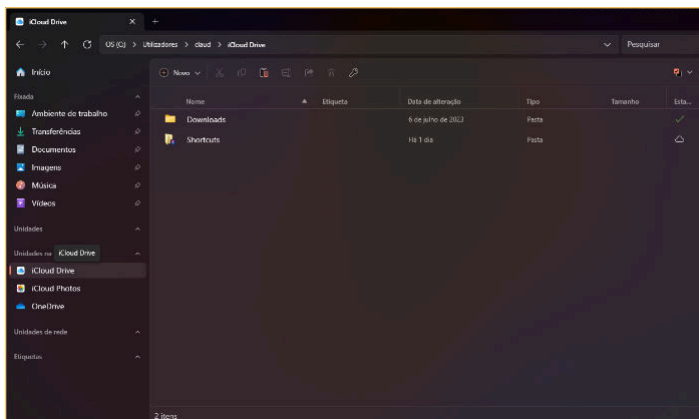
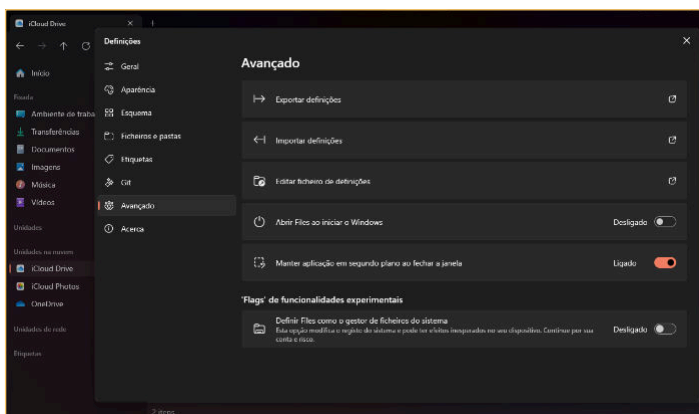
# Ofereça ferramentas incríveis ao Windows

https://tinyurl.com/bdd8fz7c

Uma das nossas ferramentas favoritas do PowerToys é o 'Peek', que permite visualizar ficheiros sem necessidade de os abrir. A versão mais recente desta suite de utilitários do sistema torna o Peek ainda mais útil ao adicionar suporte para imagens WebP e vídeos WebM. Embora estes formatos de ficheiros (desenvolvidos pelo Google) existam há anos, muitos visualizadores de imagens e leitores de vídeo não conseguem abri-los. Graças ao Peek, agora pode selecionar um ficheiro WebP ou WebM que tenha descarregado da web e pressionar Ctrl+Espaço para ver o seu conteúdo. A funcionalidade agora suporta também ficheiros de áudio, permitindo-lhe ouvir MP3s e outros formatos de áudio, sem abrir um leitor de média.
Se as pré-visualizações não estiverem a funcionar, selecione o Peek no menu principal do PowerToys e certifique-se de que a opção 'Ativar Peek' (Enable Peek) está ligada. Pode também alterar o atalho de ativação aqui.

# Descubra se a sua pendrive USB é falsa

**Comprou recentemente uma pen USB, ou uma unidade de grande capacidade (1 TB ou mais), por um preço que parecia demasiado bom para ser verdade? Infelizmente, pode muito bem acabar por ser. Há uma tendência crescente de venda de pen drives falsos na Amazon e no eBay. Estes dispositivos afirmam ter uma enorme quantidade de armazenamento - o Windows certamente pensa assim se o utilizar para verificar - mas se for um pouco mais fundo, poderá descobrir que a capacidade real é significativamente menor. Aqui, explicamos como testar a sua pen utilizando dois programas gratuitos para garantir que é realmente genuína.**

1 O primeiro programa que vamos utilizar é o ValiDrive, uma ferramenta que analisa dispositivos e unidades USB para verificar a sua capacidade real. Para tal, tenta escrever dados em todas as partes da pen e, em seguida, verifica se os dados foram efetivamente escritos no disco. Visite o sítio Web do ValiDrive em https://tinyurl.com/3m8jsret para ler um resumo do que faz e, em seguida, clique no botão verde 'Descarregar agora' para guardar o programa no seu computador.

2 Terminada a transferência, faça duplo clique no ficheiro 'validrive.exe' para iniciar o ValiDrive (é um programa portátil, pelo que não é necessário instalar). Em seguida, clique no botão 'Check USB Drive' (Verificar unidade USB) e abre-se uma janela a informar que está a ser efetuada uma verificação da unidade USB. Esta janela será substituída por uma mensagem a pedir que conecte a pen/drive que pretende verificar. Se já a tiver ligado, terá de a remover - utilize a ferramenta de ejeção na área de notificação da barra de tarefas (clique na pequena seta para baixo para a abrir) e selecione 'Ejetar disco USB'.

3 Depois de remover, o ValiDrive apresenta a seguinte mensagem: 'Acabou de ser observada uma remoção de dispositivo. Ligue o dispositivo que pretende validar'. Encaixe-o e o programa deteta e apresenta o tamanho indicado. Clique em 'Validate THIS drive' (Validar esta unidade) e o programa passa para o ecrã principal e faz a contagem decrescente para a verificação completa. Uma vez iniciada a verificação, esta ferramenta começará a escrever dados em diferentes partes da unidade e depois a lê-los. Este processo deve ser bastante rápido, mas se demorar um pouco pode indicar um problema com a pen/drive.

4 Na janela que aparece, deverá ver pontos verdes por toda a pen/drive à medida que as verificações individuais são concluídas. No entanto, se a capacidade não for a que diz, verá muitos pontos vermelhos, com apenas alguns pontos verdes a aparecerem ao longo da primeira linha da verificação. Esta situação é típica das unidades que fornecem apenas 32 GB ou 64 GB de armazenamento efetivo, embora afirmem fornecer 1 TB ou mais. Outros dispositivos baratos de 1TB podem ter a capacidade total, mas são fabricados com componentes de baixa qualidade. Estes dispositivos apresentarão uma combinação de pontos azuis e/ou amarelos para indicar erros de leitura e escrita, respetivamente. As verificações nestes dispositivos/discos de baixa qualidade demorarão muito mais tempo a ser concluídas.

5 Se for capaz de concluir uma verificação, o ValiDrive apresentará um resumo da sua análise. A menos que tudo esteja listado a verde e o 'mapa da unidade' esteja completamente verde, a unidade não está apta a ser utilizada. Se o mapa da unidade apresentar quadrados vermelhos, pode estar a indicar incorretamente a sua capacidade, ou está tão mal construída que não lê nem escreve dados corretamente. De qualquer forma, deve contactar o vendedor para obter um reembolso (não se preocupe com uma troca - irá simplesmente receber outro dispositivo falso), ou apresentar uma reclamação através do serviço onde comprou (como a Amazon ou o eBay). Neste caso, clique com o botão direito do rato na barra de tarefas e selecione Gestor de tarefas, depois selecione ValiDrive em Aplicações e clique em 'Terminar tarefa' para forçar o seu encerramento.

6 Outro sinal revelador de um dispositivo falso é o fraco desempenho. Muitos dos chamados dispositivos USB 3.0 são, na realidade, modelos USB 2.0, o que significa que está a obter velocidades de transferência que são apenas 10% das de um modelo USB 3.0 genuíno. Teste a sua velocidade utilizando a ferramenta de benchmarking gratuita CrystalDiskMark. Recomendamos a utilização da versão PortableApps - vá a https://tinyurl.com/yu7ewfey e clique na ligação 'Download from PortableApps.com' para guardar o ficheiro 'CrystalDiskMarkPortable_8.0.5.paf.exe' no seu disco rígido. Uma vez concluído, faça duplo clique no ficheiro e selecione uma pasta para o instalar. Depois disso, escolha 'Executar o CrystalDiskMark Portable' na janela que se abre e clique em Concluir.

7 Certifique-se de que a sua unidade USB está ligada a uma porta USB 3.0 ou 3.1 de cor azul. Clique no menu pendente da unidade na janela do CrystalDiskMark para selecionar a sua pen/drive e, em seguida, clique no botão 'All' (Tudo) para iniciar o teste. Aguarde enquanto um ficheiro de teste é gravado na unidade - isto pode demorar algum tempo, mas se demorar mais de cinco minutos, significa provavelmente que a unidade não é USB 3.0. Assim que os ficheiros forem criados, os testes serão executados e os resultados serão apresentados. Procure resultados de leitura SEQ1M de cerca de 125 MB/s ou superiores numa unidade USB 3.0 genuína. Se os resultados forem significativamente piores (apenas 31,79MB/s na nossa unidade de teste), então a unidade é USB 2.0 ou inferior.

# Extraia e organize ficheiros mais rapidamente

**O 'Explorador de Ficheiros' do Windows funciona bem para a maioria das tarefas, mas pensamos que a aplicação 'Files' é mais flexível. Este gestor de ficheiros de terceiros pode ser descarregado gratuitamente a partir de https://tinyurl.com/ya9fuc5v, desde que clique na ligação azul "instalador clássico" na parte inferior da página (clicar em 'Download Files' leva-o para a Microsoft Store, onde custa €8,99). A versão mais recente (3.3) está repleta de ferramentas úteis para navegar de forma rápida e eficiente no seu sistema de ficheiros e também facilita a extração e organização de ficheiros comprimidos. Explicamos as suas principais**

1 Descarregue o 'Files' e abra o programa. Primeiro, vamos dar uma vista de olhos à sua funcionalidade Smart Extract, que acelera o processo de extração de ficheiros de arquivos comprimidos ZIP, 7z e RAR. Clique num ficheiro comprimido e prima as teclas Ctrl+Shift+E - ou clique com o botão direito do rato no ficheiro, clique em 'Extrair' e depois em 'Extrair aqui (inteligente)'. Se contiver apenas um único ficheiro, este será expandido dentro da pasta atual. Se contiver vários ficheiros (ou ficheiros e subpastas), o Files criará uma nova pasta para os guardar a todos.

2 O 'Files' também facilita a compressão de ficheiros. Selecione os ficheiros que pretende incluir no seu arquivo, mantendo premida a tecla Shift ou Ctrl enquanto clica em cada um deles e, em seguida, clique com o botão direito do rato num ficheiro da sua seleção, passe o rato sobre 'Comprimir' no menu que aparece e clique em 'Criar arquivo' no sub-menu. Escreva um nome de ficheiro para o seu arquivo, depois selecione um formato e nível de compressão - 'Normal' é, na maioria das vezes, suficiente. Também pode encriptar o arquivo clicando em 'Cifra' e introduzindo uma palavra-passe no campo que aparece.

3 Alguns sistemas mais antigos têm dificuldade em lidar com ficheiros muito grandes, por isso, se for esse o caso e pretender comprimir vários gigabytes de ficheiros, deve dividi-los em partes mais pequenas. Aqui, queremos comprimir quase 9GB, por isso alterámos o Formato para '.7z', o que nos permite selecionar o tamanho máximo de cada pedaço na coleção de ficheiros resultante. Recomendamos que cada fração tenha menos de 2 GB para que seja mais fácil de gerir. Clique em 'Criar' quando estiver pronto para guardar o seu arquivo.

4 O 'Files' tem um esquema de colunas que torna a navegação nas pastas mais rápida, porque ao clicar numa pasta abre o seu conteúdo na coluna seguinte. Para mudar para este layout, clique dentro de uma pasta e, em seguida, clique no botão ‘Layout’ seguido de ‘Colunas’. Se uma pasta contiver uma subpasta, ao clicar nessa subpasta na segunda coluna abre o seu conteúdo numa terceira, e assim sucessivamente, até encontrar o ficheiro que pretende. Da mesma forma, clicar numa pasta comprimida (como um ficheiro ZIP) mostra o seu conteúdo na coluna seguinte.

5 Este programa tem também um sistema de separadores muito versátil. Prima Ctrl+T para criar um novo separador se pretender abrir duas ou mais pastas em simultâneo, ou arraste a pasta que pretende abrir para o botão do novo separador. Pode percorrer os separadores premindo Ctrl+Tab e percorrer em sentido inverso premindo Ctrl+Shift+Tab. Em alternativa, se estiver a alternar entre, por exemplo, o segundo e o quinto separadores na sua linha, utilize Ctrl+ [o número do separador]. Neste caso, seria Ctrl+2 e Ctrl+5, respetivamente. Ctrl+W fecha o separador atual.

6 O 'Files' também podem trabalhar com pastas remotas. Se tiver instalado o software para um serviço de armazenamento online como o OneDrive, pCloud ou Nextcloud no seu PC, o 'Files' reconhece-os automaticamente. Clique na seta junto a 'Unidades na nuvem' para revelar os serviços ligados. Também pode iniciar sessão num servidor FTP escrevendo o endereço do servidor na barra de endereços e iniciando sessão através da caixa que aparece.

7 O Explorador de ficheiros do Windows continuará a aparecer sempre que clicar no ícone da pasta na barra de tarefas do Windows. Se quiser alterar isso para que abra o 'Files', clique no ícone de engrenagem na barra de ferramentas ‘Files’, seguido de ‘Avançado’, e depois em 'Definir Files como o gestor de ficheiros do sistema'. Aparecerá um alerta a perguntar "Pretende permitir que esta aplicação faça alterações ao seu dispositivo?". Clique em Sim. Note que o Files avisa que isto "pode ter efeitos secundários inesperados no seu dispositivo", por isso certifique-se de que tem uma cópia de segurança completa do seu sistema antes de o fazer.